



Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

1991-09

A study of the Naval Military Personnel Command: internet connectivity issues, requirements, & recommendations

Johnson, Robert Edward; Peterson, Steven William

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/37544

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun



http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

DTIC FILE COPY

(2)

NAVAL POSTGRADUATE SCHOOL

Monterey, California

AD-A230 334

DTIC
ELECTE
JAN 0 3 1991
D
D

THESIS

A STUDY OF THE NAVAL MILITARY PERSONNEL COMMAND: INTERNET CONNECTIVITY ISSUES, REQUIREMENTS, AND RECOMMENDATIONS

by

Robert Edward Johnson
and
Steven William Peterson

March 1990

Thesis Advisor: Myung W. Suh

Approved for public release; distribution is unlimited

91 1 2 065

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b. OFFICE SYMBOL (*If applicable*) Code 54	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c. ADDRESS (*City, State, and ZIP Code*) Monterey, California 93943-5000	7b. ADDRESS (*City, State, and ZIP Code*) Monterey, California 93943-5000
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (*If applicable*)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (*City, State, and ZIP Code*)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO.

11. TITLE (*Include Security Classification*) A STUDY OF THE NAVAL MILITARY PERSONNEL COMMAND: INTERNET, ISSUES, REQUIREMENTS, AND RECOMMENDATIONS (UNCLASSIFIED)

12. PERSONAL AUTHOR(S) Johnson, Robert E.; Peterson, Steven W.

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (*Year, Month, Day*)	15. PAGE COUNT
Master's Thesis	FROM _____ TO _____	March 1990	225

16. SUPPLEMENTARY NOTATION The views expressed in this thesis are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17. COSATI CODES		
FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS (*Continue on reverse if necessary and identify by block number*)
internetwork connectivity, local area networks, Naval Military Personnel Command, OSI Model, IEEE Standards, GOSIP protocols, DECnet, Novell Netware, HYPERbus network

19. ABSTRACT (*Continue on reverse if necessary and identify by block number*)

This thesis is a study of the Naval Military Personnel Command (NMPC) and its requirements to interconnect office area/local area networks and mainframe resources to form a comprehensive, organization-wide internet. The paper serves three purposes: it examines NMPC's organizational environment and internet requirements, proposes alternative internet configurations and recommendations, and uses information systems management lessons learned in studying NMPC to make internet planning recommendations of use to other Department of Defense organizations. It is written with the assumption that the reader is familiar with local area networks and accepted government and industry standardization guidelines; however, a series of detailed appendices covering these subjects is provided as an aid to the unfamiliar reader.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION Unclassified
22a. NAME OF RESPONSIBLE INDIVIDUAL Myung W. Suh	22b. TELEPHONE (*Include Area Code*) (408) 646-2637 22c. OFFICE SYMBOL Code 54Su

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted. All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

☆ U.S. Government Printing Office: 1988—606-24.

Approved for public release; distribution is unlimited

A Study of the Naval Military Personnel Command:
Internet Connectivity Issues, Requirements, & Recommendations

by

Robert Edward Johnson
Lieutenant, United States Navy
B.S., University of Kansas, 1984

and

Steven William Peterson
Captain, United States Army
B.S., United States Military Academy, 1982

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
March 1990

Authors: [redacted]
Robert E. Johnson

[redacted]
Steven W. Peterson

Approved by: [redacted]
Myung W. Suh, Thesis Advisor

[redacted]
Magdi N. Kamel, Second Reader

[redacted]
David R. Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

This thesis is a study of the Naval Military Personnel Command (NMPC) and its requirements to interconnect office area/local area networks and mainframe resources to form a comprehensive, organization-wide internet. The paper serves three purposes: it examines NMPC's organizational environment and internet requirements, proposes alternative internet configurations and recommendations, and uses information systems management lessons learned in studying NMPC to make internet planning recommendations of use to other Department of Defense organizations. It is written with the assumption that the reader is familiar with local area networks and accepted government and industry standardization guidelines; however, a series of detailed appendices covering these subjects is provided as an aid to the unfamiliar reader.

Accesion For
NTIS CRA&I
DTIC TAB
Unannounced
Justification
By
Distribution /
Availability Codes
Dist | Avail and / or Special
A-1

TABLE OF CONTENTS

I. INTRODUCTION 1

A. PURPOSE 1

B. RESEARCH METHODOLOGY 1

C. ORGANIZATION 2

II. NMPC MISSION AND ORGANIZATION 4

A. INTRODUCTION 4

B. NMPC AND THE DEPARTMENT OF THE NAVY MPT ORGANIZATION . . . 4

C. NMPC MISSION 6

D. ORGANIZATION 6

E. THE NMPC ORGANIZATION & INFORMATION SYSTEMS DEVELOPMENT. . 12

III. CNP COMPONENT INFORMATION RESOURCES MANAGEMENT PLAN 13

A. INTRODUCTION 13

B. PURPOSE OF THE CNP CIRMP 14

C. PHASES OF THE MPT IRM PROGRAM 14

D. THE ROLE OF NETWORKS IN THE CNP CIRMP 17

IV. CNP TECHNICAL ARCHITECTURE PLAN 20

A. INTRODUCTION 20

B. SCOPE AND CONTENTS OF THE CNP TAP 20

C. TYPES OF TECHNICAL ARCHITECTURES 22

D. PLANNING FACTORS 23

E. THE CNP TAP AND NMPC'S TECHNICAL ARCHITECTURE 28

F. THE CNP TAP AND CNP CIRMP IN NMPC INTERNET DEVELOPMENT. . 29

V. INTERNET FUNCTIONALITY REQUIREMENTS 30

A. INTRODUCTION 30

B. FUNCTIONAL REQUIREMENTS OF DEPARTMENTAL OAN'S 30

C. INTERNET FUNCTIONAL REQUIREMENTS 33

VI. NMPC NETWORKS AND RESOURCES 35
A. INTRODUCTION 35
B. EVOLUTION OF NMPC'S BASELINE ARCHITECTURE 36
C. IBM MAINFRAMES 37
D. HYPERBUS LAN 37
E. DEC NETWORKS 40
F. NOVELL NETWORKS 42
G. THE MAPTIS GRID 43
H. A COMPREHENSIVE NMPC INTERNET 45
VII. POTENTIAL GATEWAYS AND BRIDGES FOR AN NMPC INTERNET 47
A. INTRODUCTION 47
B. HYPERBUS CONNECTIVITY 47
C. DECNET CONNECTIVITY 61
D. DEVELOPING ALTERNATIVES FOR AN NMPC INTERNET 67
VIII. INTERNET ALTERNATIVES AND RECOMMENDATIONS 68
A. INTRODUCTION 68
B. ALTERNATIVE 1: NOVELL OAN'S - HYPERBUS - DECNETS . . . 68
C. ALTERNATIVE 2: NOVELL OAN'S - HYPERBUS - DECNET BACKBONE - DECNETS 73
D. ALTERNATIVE 3: NOVELL/DECNETS - DECNET BACKBONE - IBM'S 78
E. CHARACTERISTICS COMMON TO ALTERNATIVES 1, 2, AND 3 . . . 82
F. INTERNET RECOMMENDATIONS 84
IX. NETWORK PLANNING AND DEVELOPMENT IN NMPC 86
A. INTRODUCTION 86
B. ORGANIZATIONAL RESPONSIBILITY 87
C. NETWORK PLANNING 88
X. IS MANAGEMENT RECOMMENDATIONS 91
A. INTRODUCTION 91
B. THE STATUS QUO 91
C. STRENGTHS AND WEAKNESSES OF THE STATUS QUO 92
D. RECOMMENDATIONS 97

XI. LESSONS LEARNED IN STUDYING NMPC 100
A. INTRODUCTION 100
B. EFFECTIVENESS OF STRATEGIC PLANS 100
C. PITFALLS IN IMPLEMENTATION OF INFORMATION SYSTEMS 102
D. THE VALUE OF ADHERING TO STANDARDS 104
E. APPLYING NMPC LESSONS 105
XII. RECOMMENDATIONS FOR INTERNET PLANNING AND DEVELOPMENT 107
A. INTRODUCTION 107
B. IDENTIFYING REQUIRED FUNCTIONALITY 107
C. IDENTIFYING HARDWARE/SOFTWARE & CONNECTIVITY REQUIREMENTS 109
D. IMPLEMENTING THE INTERNET 111
E. SUMMARY OF THE STEPS RECOMMENDED IN BUILDING AN INTERNET. 111
APPENDIX A: NMPC ORGANIZATION AND IRM RESPONSIBILITIES 114
APPENDIX B: LOCAL AREA NETWORKS 119
APPENDIX C: INTERNATIONAL STANDARDS ORGANIZATION OPEN SYSTEMS INTERCONNECTION MODEL 137
APPENDIX D: IEEE STANDARDS 145
APPENDIX E: GOVERNMENT OPEN SYSTEMS INTERCONNECTION PROFILE . . . 150
APPENDIX F: BUILDING AN INTERNET 157
APPENDIX G: CHARACTERISTICS OF SELECTED COMMERCIAL NETWORKS . . . 169
APPENDIX H: SUMMARY OF NMPC OAN'S/LAN'S & FUNCTIONAL REQUIREMENTS. 206
APPENDIX I: GLOSSARY OF ACRONYMS AND TERMS 207
LIST OF REFERENCES 213

LIST OF TABLES

1 SUMMARY OF HYPERBUS SPECIFICATIONS 38

2 COMPARISON OF DECNET AND HYPERBUS ARCHITECTURES 59

A-1 SUMMARY OF NMPC IRM RESPONSIBILIITES 118

B-1 COMPARISON OF TRANSMISSION MEDIA 135

B-2 COMPARISON OF BASIC TOPOLOGIES 136

D-1 PHYSICAL LAYER ALTERNATIVES OF IEEE 802.3 148

LIST OF FIGURES

1	NMPC RELATIVE TO THE CNP MPT STRUCTURE	5
2	NMPC ORGANIZATION	7
3	NMPC-16 ORGANIZATION	9
4	ORGANIZATIONAL SCOPE OF CNP TAP	21
5	NMPC'S BASELINE SYSTEMS	35
6	POTENTIAL NMPC SYSTEM-TO-SYSTEM CONNECTIONS	46
7	COMPARISON OF HYPERBUS AND NOVELL FRAME FORMATS	54
8	DECNET FRAME FORMAT	59
9	ALTERNATIVE 1 (NOVELL OAN'S - HYPERBUS - DECNETS)	69
10	ALTERNATIVE 2 (NOVELLS - HYPERBUS - DECNET BACKBONE - DECNETS)	74
11	ALTERNATIVE 3 (NOVELL/DECNET'S - DECNET BACKBONE - IBM'S)	79
B-1	BUS TOPOLOGY	128
B-2	RING TOPOLOGY	130
B-3	STAR TOPOLOGY	131
C-1	SEVEN LAYERS OF THE OSI REFERENCE MODEL	139
D-1	COMPARISON OF IEEE 802 AND OSI LAYERS 1 AND 2	146
D-2	THREE LAYERS OF IEEE 802	149
E-1	GOSIP PROTOCOLS	154
F-1	BRIDGE	161
F-2	GATEWAY	164
F-3	GATEWAY FRAME CONVERSION	166
G-1	DECNET IV - OSI LAYERS	173
G-2	NETWARE FILE SERVER SHELL	185
G-3	NETWARE AND THE ISO OSI MODEL	186
G-4	NETWARE COMMUNICATIONS LAYERS	188
G-5	HYPERBUS COMPONENTS	197
G-6	HYPERBUS MULTIPLE BUS CONFIGURATION	201
G-7	HYPERBUS ADDRESSING FORMATS	203

I. INTRODUCTION

A. PURPOSE.

This work is the result of a study of the Naval Military Personnel Command (NMPC) and it's requirements to interconnect office area/local area networks and mainframe resources to form a comprehensive, organization-wide internet. The paper serves three purposes: it examines NMPC's organizational environment and internet requirements, proposes alternative internet configurations and recommendations, and uses information systems management lessons learned in studying NMPC to make internet planning recommendations of use to other DOD organizations.

B. RESEARCH METHODOLOGY.

The research performed in producing this study concentrated on four principal sources of information:

- Scholarly literature and technical documentation for local area networks and government/industry networking standards.
- On-site survey of NMPC's facilities located in the Navy Annex, Arlington, Virginia and interviews with key technical and managerial personnel of NMPC-16, the Total Force Information Systems Management Department.
- Chief of Naval Personnel/NMPC information systems plans, policies, and governing directives.

- Review of systems documentation and information supplied by commercial vendors of network/interconnectivity products applicable to NMPC's requirements.

C. ORGANIZATION.

The results of the study are organized and presented as follows. The first four chapters examine the NMPC mission and organizational environment with particular emphasis on the principal planning documents which guide information Systems development within NMPC. Chapters 5 through 8 discuss the functionality required of an NMPC internet, introduce the resources to be connected, discuss technical aspects of achieving connectivity between diverse systems, and make recommendations for alternative internet architectures. The fina chapters of the study review managerial aspects of network planning and internet development within NMPC and make recommendations for other DOD organizations facing internet development decisions.

The study is written with the assumption that the reader is familiar with local area networks and accepted government and industry standardization guidelines. A series of detailed appendices are provided to aid the reader who is unfamiliar with these subjects. Appendix A provides an overview of information resource management responsibility in NMPC. Appendix B discusses local area networks in general. Appendix C reviews the International Standards Organization Open Systems Interconnection Model (ISO/OSI). Appendices D and E further explore open systems standardization guidelines by examining the IEEE

standards for local area networks and introducing the United States Government Open Systems Interconnection Profile. Appendix F discusses the technical aspects of gateways and bridges, the two most common devices used to build an internet. Appendix C introduces the architectures of the networks found within NMPC. Appendix H provides a summary of NMPC's LAN functionality requirements and Appendix I is a glossary of terms used throughout the paper.

II. NMPC MISSION AND ORGANIZATION

A. INTRODUCTION.

In order to effectively address the internetworking requirements of the Naval Military Personnel Command (NMPC), one must first understand its mission, organization, and role in the Department of the Navy. This chapter provides an overview of NMPC and gives a brief discussion of each of its organizational elements. Particular emphasis is placed on the role of the Total Force Information Systems Management Department (NMPC-16), since it not only manages network planning and development within NMPC but is also responsible for information resources management throughout the Navy's entire Manpower, Personnel, and Training (MPT) structure.

B. NMPC AND THE DEPARTMENT OF THE NAVY MPT ORGANIZATION.

To understand the mission and organization of NMPC, one must first recognize the placement of NMPC in the Department of the Navy's organization. Since NMPC serves multiple roles within DON, one cannot define and address its internetworking requirements without a thorough understanding of its multifaceted organizational nature.

Within the Navy's Manpower, Personnel and Training (MPT) structure, many of the organizational elements, including NMPC, are dual or triple "hatted". In

other words, key leaders and organizational elements simultaneously serve DON or Chief of Naval Personnel headquarters staff roles as well as Navy-wide roles. Understanding NMPC's multiple roles is critical to understanding the complex functionality requirements of its information systems, particularly its internet/gateway needs. Figure 1 depicts the organization of the Chief of Naval Operations' staff element, OP-01, showing the placement of NMPC in the MPT structure.

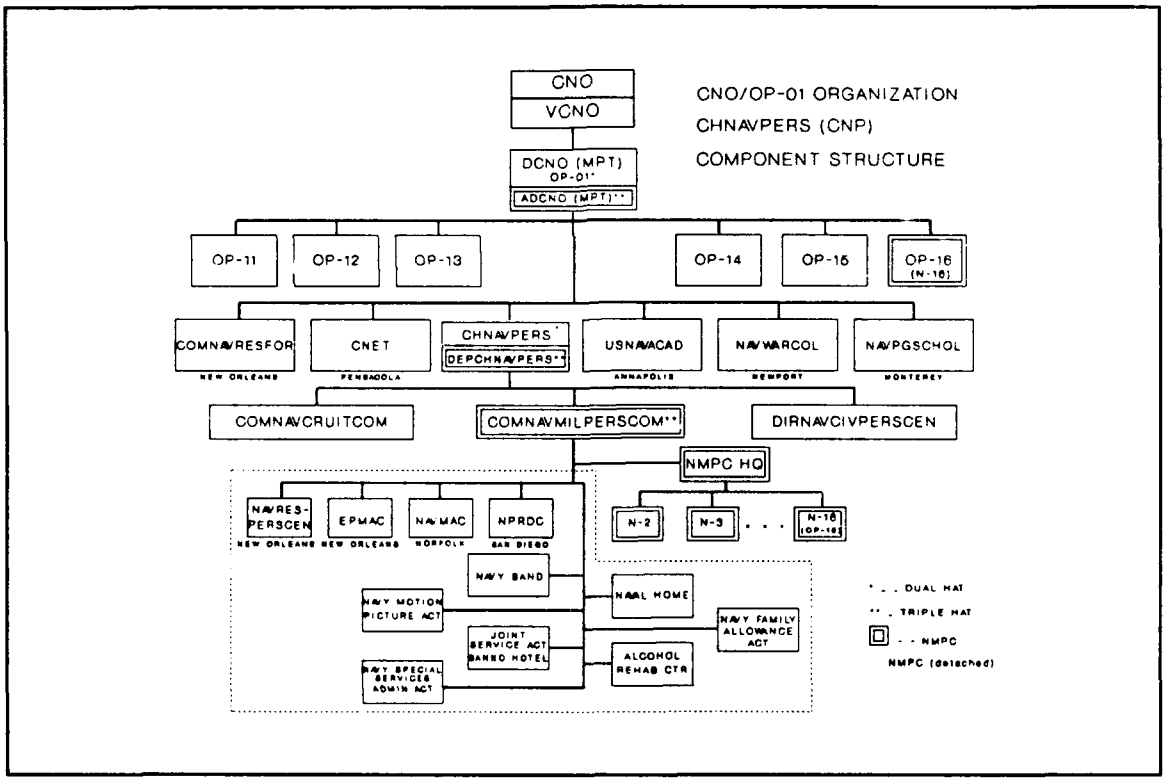


Figure 1: NMPC Relative to the CNP MPT Structure

OP-01 is responsible for staff supervision of all of the Navy's MPT programs. It is headed by the Deputy Chief of Naval Operations MPT (DCNO MPT) who also serves as the Chief of Naval Personnel (CNP). Directly under the DCNO MPT is the Assistant Deputy Chief of Naval Operations MPT (ADCNO MPT) who serves three roles: Assistant DCNO MPT, Deputy Chief of Naval Personnel, and Commander Naval Military Personnel Command. This organization requires that NMPC information systems be capable of meeting decision making and management needs at three levels: Department of the Navy, Chief of Naval Personnel, and internal to NMPC.

C. NMPC MISSION.

NMPC controls the duty assignment, utilization, education, and promotion of all Navy military personnel. It administers all personnel programs for the Navy's 501,000 active duty and 174,000 reserve personnel, manages related funding appropriations, and serves as the Chief of Naval Personnel's proponent for information systems management. To perform these functions, NMPC is organized into several administrative sections and eleven major departments.

D. ORGANIZATION.

Figure 2 shows the organizational structure of NMPC. Each of its elements is described in Appendix A. The functions of NMPC-16, the Total Force Information Systems Management Office, are discussed below.

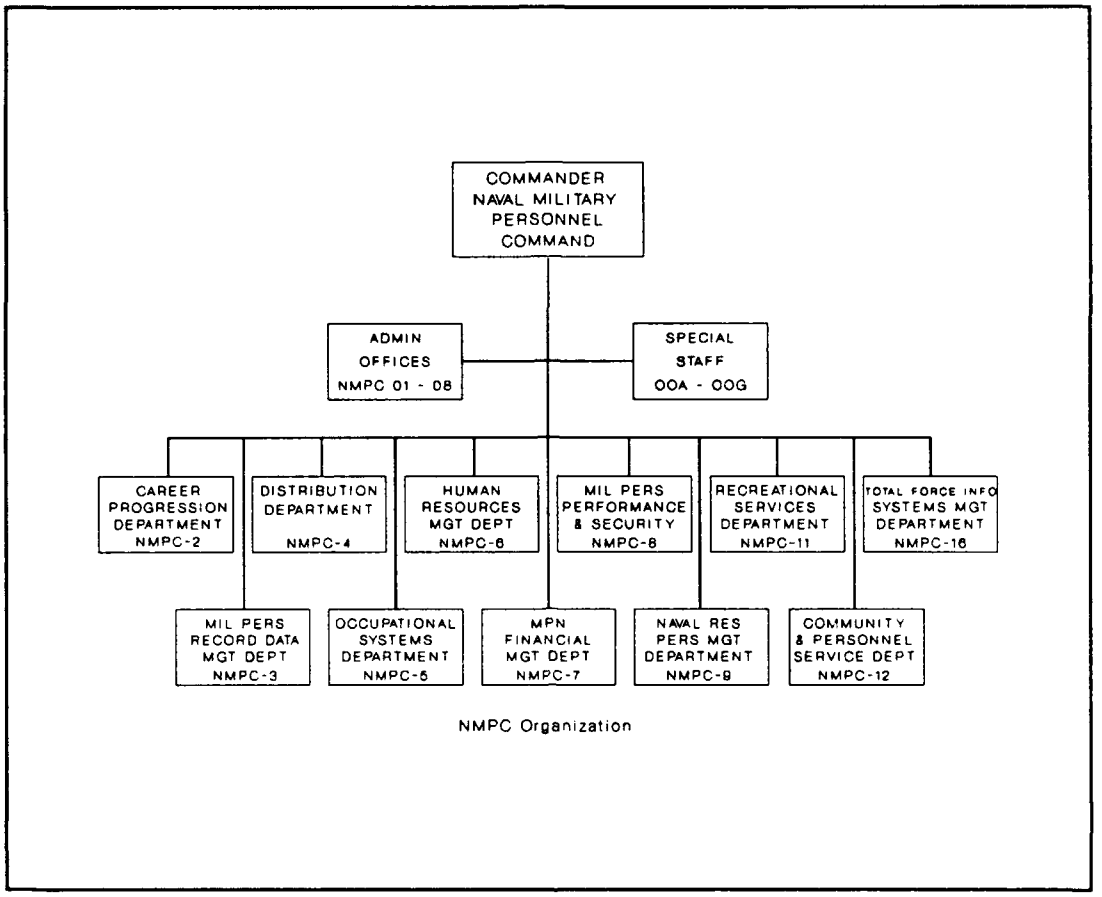


Figure 2: NMPC Organization

1. NMPC-16, Total Force Information Systems Management Department.

NMPC-16 is responsible for all facets of NMPC's internal information systems planning and management including ADP security, information resource management, data administration, life cycle management, quality assurance, systems architecture, and ADP resource allocation functions. In addition to its NMPC functions, NMPC-16 has two other roles. First, it is a component of the OPNAV staff (designated OP-16, the Total Force Information Resources

Management Division) and as such is responsible for the implementation of the Navy's overall MPT Information Resources Management Program. Second, it serves as the Chief of Naval Personnel Claimancy's executive agent for Manpower, Personnel, and Training Information Systems (MAPTIS) programs.

Figure 3 on the following page shows the organization of NMPC-16. A basic knowledge of its organization is essential to understanding the findings and recommendations presented in this paper. Accordingly, each of its organizational elements is briefly described here.

a. Director, NMPC-16

The Director is triple-hatted, serving also as the Director, OP-16, and performing NMPC staff functions for the Chief of Naval Personnel.

b. NMPC-16B, Deputy Director

The Deputy Director assists the director in the management of NMPC-16; monitors program execution throughout the department; overseas strategic planning functions; coordinates department-wide initiatives; ensures compliance with higher level policy directives and implementation of the CNP Component Information Resources Management Plan.

c. NMPC-16C, Administrative Support Office

This office handles the department's military personnel matters, space utilization, and various administrative support functions.

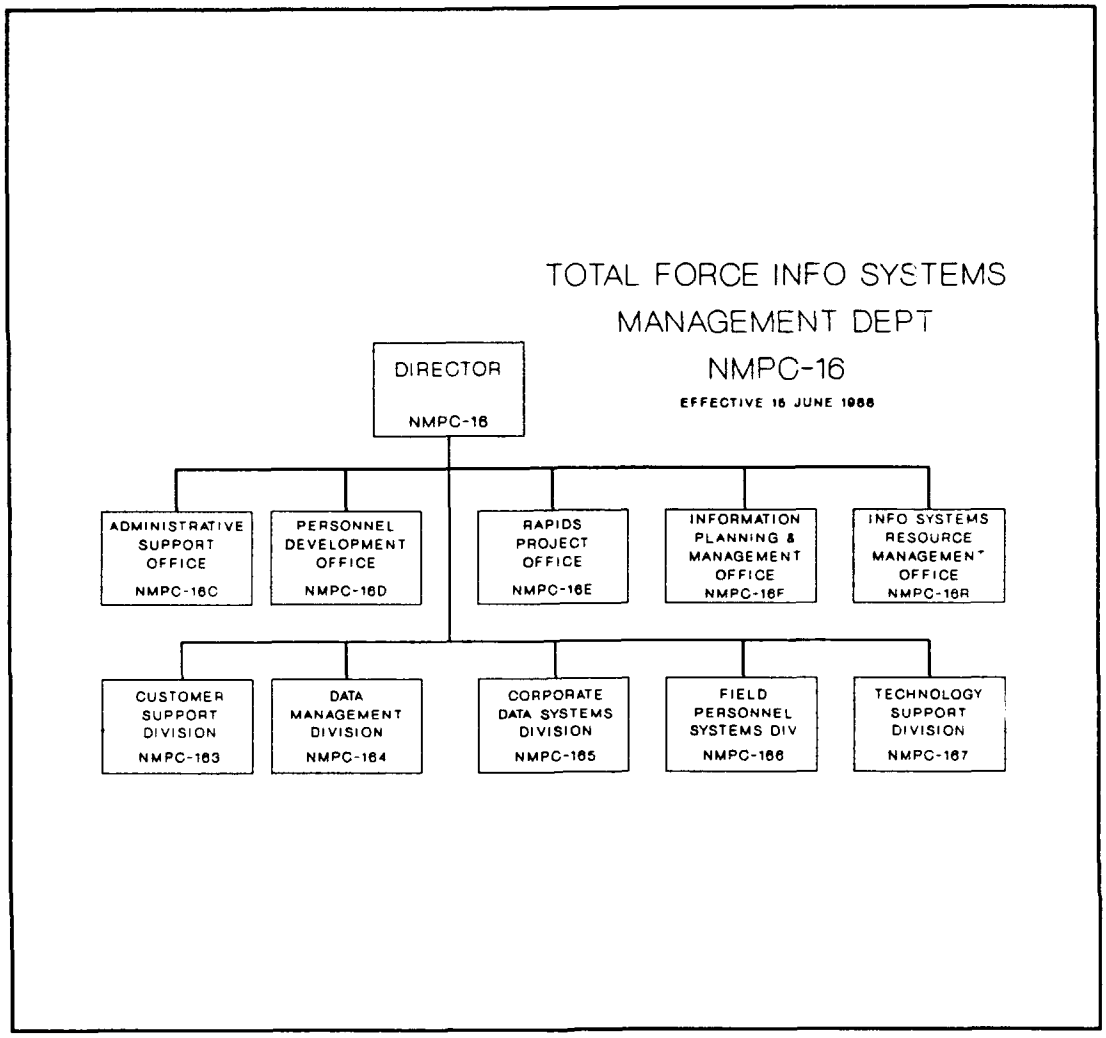


Figure 3: NMPC-16 Organization

d. NMPC-16D, Personnel Development Office

This section is responsible for managing the department's positions/billets, civilian personnel issues, and personnel training programs.

e. NMPC-16E, RAPIDS Project Office

The RAPIDS Office administers the Realtime Automated Personnel Identification System (RAPIDS) project. RAPIDS is a DOD system development

initiative which Department of the Navy has been tasked with administering. This office was created within NMPC-16 (in its role as OP-16) specifically to carry out the DON level staff functions associated with this program and is a good example of how NMPC's multiple roles affect it's internal organization and correspondingly its information systems requirements.

f. NMPC-16F, Information Planning and Management Office

This office administers the information resources management process for the Chief of Naval Personnel. It's responsibilities include IRM planning, lifecycle management, and data management policy formulation.

g. NMPC-16R, Information Systems Resource Management Office

This section is responsible for the planning, programming, budgeting, and execution of resources necessary to provide adequate information systems support of NMPC operations.

h. NMPC-163, Customer Support Division

This division is responsible for translating the needs of MPT functional managers within CNP, OP-01, and NMPC staffs and line organizations into effective information systems. This includes planning, designing, specifying and implementing information systems as well as managing the process from initial identification of need through contracting, installation, and training. Much of the research supporting this paper was obtained through interviews with key personnel within this division. NMPC-163 plays a critical role in the

identification of NMPC's internet functionality requirements and will ultimately be responsible for implementation of recommended gateway solutions.

i. NMPC-164, Data Management Division

This division administers ongoing efforts to ensure a clear definition of MPT data requirements and ensure data integrity, reliability, security, and accuracy while allowing responsive, timely access sufficient to meet the needs of MPT functional managers.

j. NMPC-165, Corporate Data Systems Division

This section is responsible for the development and management of centralized repositories of Navy-wide data for the total Naval force of both civilian and military manpower. These systems support DON, DOD, and higher management information requirements.

k. NMPC-166, Field Personnel Systems Division

This office conducts planning, design, development, implementation, and maintenance of Navy-wide information systems which deal with matters of civilian and military personnel to include interfaces in support of pay systems. Its responsibilities include pay offices and field personnel as well as related headquarters organizations' information systems.

l. NMPC-167, Technology Support Division

This division handles all aspects of design, planning, implementation, operation, integration, and maintenance of computer processing and telecommunications resources in support of Navy MPT requirements. It will

have primary technical responsibility for implementing solutions to NMPC's internet functionality/ gateway requirements and accordingly was a key resource in the research supporting this study. As the technical experts on NMPC information systems networks, key personnel from this office were extensively interviewed to determine the capabilities and constraints of existing and planned network resources. Their input weighed heavily in the evaluation of alternative internet solutions and the formulation of gateway recommendations made in Chapter 8 this paper.

E. THE NMPC ORGANIZATION & INFORMATION SYSTEMS DEVELOPMENT.

NMPC's organization and the multiple levels upon which it is tasked to perform MPT support functions clearly suggest a requirement for complex information systems planning and development. NMPC-16's efforts in this area are governed by the guidance contained in the Chief of Naval Personnel Component Information Resources Management Plan -- the subject of the next chapter.

III. CNP COMPONENT INFORMATION RESOURCES MANAGEMENT PLAN

A. INTRODUCTION.

In this period of shrinking budgets and competing priorities, the careful management of information systems resources is critical. Recognizing this, the Department of the Navy has established management guidelines in response to which the Chief of Naval Personnel has issued the Chief of Naval Personnel Component Information Resources Management Plan (CNP CIRMP). This document is significant to NMPC in two ways. First, NMPC must comply with the information resource management strategy it outlines. Second, as OP-16, NMPC-16 is responsible for overseeing the execution of the CNP CIRMP. Accordingly, a basic understanding of its requirements is necessary to establish the constraints under which the internet/gateway recommendations presented in Chapters 7 and 8 were developed.

This chapter first briefly summarizes the CNP CIRMP then analyzes it in terms of the internetworking requirements it suggests. In some areas, the plan clearly acknowledges the need for network development and internet connectivity. But more significantly, a careful study of the plan's requirements leads to the implicit conclusion that a high level of dependence upon networks is a necessary, perhaps inevitable, consequence of the plan.

B. PURPOSE OF THE CNP CIRMP.

The CNP CIRMP is a document which summarizes into a single coherent plan all of the goals, objectives, and strategies to be followed by the CNP Claimancy during the next six years. Its goal is to achieve an environment of effective information resources management through sound program initiatives. The heart of the document is the CNP IRM Program Six Year Scenario which prioritizes CNP IRM activities, serves as a planning tool for the budgeting process, and provides information "concerning the interfaces among information systems and programs." [Ref. 1:p. i]

C. PHASES OF THE MPT IRM PROGRAM.

The MPT IRM program is being implemented in three phases. First, is the Technology and Automated Information Systems Phase completed in 1985. According to the plan, "This phase was characterized by an investment of significant energy and resources to modernize the hardware, software and communications technology infrastructure. Major hardware procurements have revitalized obsolete equipment and installed numerous microcomputers in a number of commands." [Ref. 1:p. 2-1].[1]

[1]Research findings seem to contradict the plan's conclusion that the objectives of the AIS phase were fully met in 1985. Although obsolete equipment was indeed replaced and microcomputers proliferated, there is little evidence that a communications infrastructure capable of meeting the long term internetworking needs of the command was developed.

The second phase, is the Data and Technology Phase. Begun in 1986, it is the current phase of the program. The plan states that "Great progress is being made in standardizing MPT data and developing integrated Total Force data structures to provide a centralized, common source of data, facilitate distributed processing and foster user independence." [Ref. 1:p. 2-3]. The Data/Technology Strategy phase is defined as an "orientation that data requirements drive functional requirements and the application of technology" [Ref.1:p. i]. It is marked by an emphasis on distributed systems in the form of initiatives aimed at the effective development of "departmental and end-user computing" [Ref. 1: p. i].

Corporate data processing initiatives are also a significant part of this phase. A major effort is underway to clearly define data requirements for common corporate databases to be used throughout the Navy's entire MPT organization. These databases will be fed by departmental systems and yet provide a data view useful to strategic decision makers at the CNP, DON, DOD, and higher levels. This requires a proactive approach to information systems management. Specifically, it will be necessary to increase the ability of line managers in the field and headquarters staff members to capture, access, and share data in an accurate and timely manner. [Ref. 1:pp. i-vii]

According to the CNP CIRMP, the roles of ADP and MIS personnel in the organization are evolving. Technological advances in corporate database management and executive information systems will allow top-level management

to exert greater influence and control over the organization and conduct of business. End-users will continue to become more computer literate and take the lead in solving their own information requirements. This will require a change in organization and emphasis of MIS activities toward a support role and away from centralized control. The plan encourages this shift while recognizing that there will be a need for measures to "facilitate compatibility, interoperability, communications, and data standards" [Ref. 1:p. iii]. This suggests that the increase in end-user computing and the development of departmental systems will require careful planning of internetwork connectivity to meet corporate data requirements crossing departmental lines.

The Data/Technology phase is expected to end in 1992 with the beginning of the Chief Information Officer Phase and the establishment of a new organizational perspective on information resources. This phase will begin with the creation of an MPT Chief Information Officer (CIO). The CIO will be an individual who has a thorough understanding of both the business operations and information systems capabilities of the MPT community. He will play a key role in strategic policy formulation and ensure that information is used effectively as a corporate resource. The CIO Phase will also be "identified by the integration of IRM data planning with MPT business planning and by widespread information sharing across systems and organizations. Data and technological structures will be in place to provide maximum productivity and efficiency in the use of MPT data." [Ref. 1: p. 2-3].

D. THE ROLE OF NETWORKS IN THE CNP CIRMP.

The CNP CIRMP encourages the extensive development of end-user computing, the development of comprehensive corporate databases, and the sharing of data/resources across NMPC and other organizations of the Navy's MPT structure. Network development and internetwork connectivity are not extensively addressed within the CNP CIRMP. However, analysis of its stated principles and goals suggests they will play a necessary role in implementation of the plan. To demonstrate the validity of this conclusion, the statements shown in italics below are "guiding principles" extracted directly from the CNP CIRMP [Ref. 1:pp. vi-vii, 1-17]. Each is followed by analysis supporting the use of local area networks and internetworking to meet the plan's overall goals.

> *Data will be collected and entered only once. Redundant collection will only be authorized for specific functions such as verification.*

> *Official information should be retained in only one place unless multiple storage locations are specifically authorized for meeting the MPT mission, or for security, integrity, privacy, or efficiency reasons. Clearly, data redundancy will be planned.*

These principles reinforce CNP's efforts to define and build effective corporate databases. However, simultaneously the CNP CIRMP's stated goal of fostering end-user computing through the development of departmental systems seems to conflict with this effort at centralization of data. The answer to this dilemma lies in the effective internetworking of separate departmental systems. Although each department has unique information requirements, they share some universal data elements which should be maintained in a corporate database.

Through local networking each department may maintain its unique data and perform processing functions tailored to its needs; while effective internetworking can allow it to access or update the corporate database as required. In this manner, data can be captured as it is developed by each department and integrated with the corporate database where appropriate. This solution has the added benefit of meeting the following CNP CIRMP principles as well.

Both editing of data inputs and correction of input errors should be performed at the input source to the maximum extent possible.

Data will be placed as close to the end user as possible.

Development and use of departmental systems helps guarantee both the accuracy of data inputs as they are captured as well as allowing data to be maintained as close as possible to its principle users. Thus, "Responsiveness is increased when processing of transactions is carried out at their points of occurrence."[Ref. 3:p. 197] and data integrity/redundancy problems can be reduced by using internetworking to tie departmental systems into applicable corporate databases. Furthermore, the use of internets is consistent with the CNP CIRMP's call for the sharing of data and resources.

IRM resources will be shared to the maximum extent possible.

Achieve increased information sharing and cooperation across org nizational boundaries both within and outside of OP-01.

Information and resource sharing is perhaps the foremost justification for the use of networks and internetworking [Ref. 3: pp. 160-161]. Therefore the

development of LAN's and internets appears a logical way of meeting the goals of the plan. However, the communications infrastructure and technical solutions necessary to effectively interconnect diverse departmental systems are not yet in place throughout NMPC or other elements of the Navy's MPT structure. Fortunately, the authority to pursue the development of such solutions is compatible with the CNP CIRMP which specifically states that

Appropriate technological improvements will be effected based on need.

It is obvious from the above discussion that the stated IRM goals of the CNP claimancy correspond very well to commonly accepted arguments for distributed systems, the use of networks and internetworking. However, concrete provisions for implementing such systems within NMPC and other elements of the Navy's MPT structure are not obvious from the CNP CIRMP alone. Therefore, before one can effectively address NMPC's specific internetworking requirements it is necessary to examine The Chief of Naval Personnel Technical Architecture Plan (CNP TAP).

IV. CNP TECHNICAL ARCHITECTURE PLAN

A. INTRODUCTION.

NMPC-16 manages the Chief of Naval Personnel Technical Architecture Plan (CNP TAP).[2] It outlines the technical architecture to be used in achieving the goals of the CNP Component Information Resources Management Plan (CNP CIRMP). NMPC has two roles reference the CNP TAP. First, it is responsible for executing the plan in the development and implementation of its internal systems. Second, in its OPNAV staff role, it manages the technical architecture for the entire CNP claimancy. This makes the plan of critical significance in the definition of network and internetwork requirements for NMPC.

This chapter briefly describes pertinent aspects of the plan in order to form a frame of reference for the discussion of internetwork connectivity requirements and recommendations set forth in this paper.

B. SCOPE AND CONTENTS OF THE CNP TAP.

Figure 4 defines the scope of organizations covered by the CNP TAP. The plan outlines the major systems and processing centers which now exist within the CNP Claimancy and discusses the technical architecture planning

[2]NMPC-167, the Technology Support Division, produced the plan.

methodology, strategy, and initiatives to be followed in reaching the Target Technical Architecture it defines.

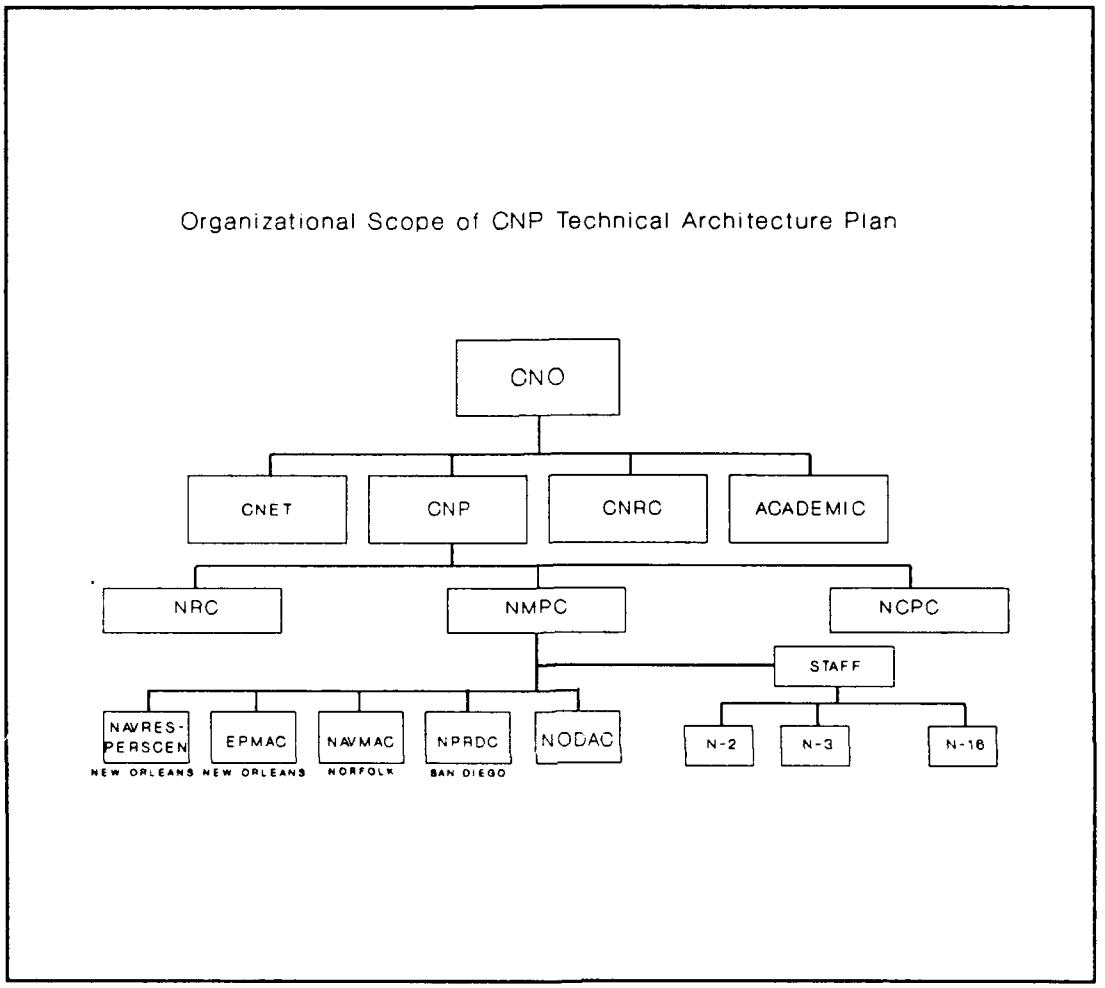


Figure 4: Organizational Scope of CNP TAP

The purpose of the CNP TAP is

> [to outline] the technical strategies, policies and programs that the CNP claimancy will implement to improve MPT mission performance through application and sharing of MPT information resources over the next six to ten years. [Ref. 4:p. iii]

C. TYPES OF TECHNICAL ARCHITECTURES.

The plan discusses technical architectures in three time frames: a baseline architecture, a transition architecture, and a target architecture. The baseline architecture defines the systems and resources that currently exist. The transition architecture looks one to two years in the future and discusses those systems and resources that are presently planned. The target architecture is a view of three to eight years in the future and corresponds to outyear planning in the programming and budgeting process. [Ref. 4:p. 25]

In each of these time frames, the CNP TAP discusses three types of technical architectures: communications, database/applications, and facilities architectures. The communications architecture deals with wide area networks, the Defense Data Network (DDN), dedicated/dial-up circuits, and communications protocols. The database/applications architecture covers automated information systems, corporate databases, data distribution, and the interrelationships of these components across the facilities architecture. The facilities architecture addresses mainframe hardware and software, data processing, local area networks, office automation, departmental computing, and end-user computing initiatives. [Ref. 4:p. 25] When addressing NMPC's internetwork connectivity requirements, the facilities and communications architectures are directly significant while the database/applications architecture indirectly influences internet issues.

D. PLANNING FACTORS.

The CNP TAP defines six key factors which appropriately influence technical architecture planning. These are user requirements, capacity requirements, baseline architecture, resources, technology, and standards/guidance. They represent constraints which must be considered in all IS planning and proved particularly important in the study of NMPC's internetwork connectivity requirements. Because of their significance in reaching the conclusions and recommendations presented in Chapter 8 of this paper, the discussion of each factor presented below is of greater scope than that found in the CNP TAP.

1. User/Data Requirements.

The ultimate goal of any information system is to be responsive to the needs of its users by providing timely, accurate, effective support. In order to develop an effective technical architecture one must first clearly define the user's IS requirements. The work a user seeks to accomplish and the types of data to be communicated and manipulated are critical aspects of a system's design. For example, a user requiring batch transaction processing of primarily numerical data will have much different system requirements than a user who needs an interactive interface with the modeling capabilities of advanced decision support. Similarly, users with complex data transmission needs, such as voice and video, will require vastly different network communications provisions than users with "conventional" data needs. When an organization's

users have such diverse IS needs, careful planning is required to produce a technical architecture which effectively meets both individual and corporate requirements.

2. Capacity Requirements.

In planning a technical architecture, care must be taken to insure that it will have sufficient capacity to meet projected user requirements. This means adequate processing power, user access, data storage and communications capabilities must be considered in developing an organization's transition and target architectures. Growth in the number of users and the complexity of their requirements must be anticipated. Achieving a working information system only to find that the needs of the organization have expanded beyond its capabilities during the time it took to design, procure, and implement is a common pitfall of systems development. Technical architectures that allow for growth and have planned expansion flexibility are essential if an organization's information systems are to keep pace with organizational change.

3. Baseline Configuration.

Existing hardware, software, and communications infrastructure form the starting point for technical architecture planning in an organization. Existing systems represent significant resource commitments which few organizations can afford to ignore when planning for the future. The most cost effective future options are normally a result of incorporating existing systems. As a result, baseline systems significantly influence the nature of the target

architecture. Frequently, this approach leads to effective systems development, however, it also has the potential to produce disaster. Decision makers who face restricted budgets and fierce competition for scarce resources sometimes ignore the benefits of sunk cost planning and succumb to the temptation to accept cheaper, interim fixes rather than seeking long term solutions. This results in a gradual overloading of existing resources and a piecemeal, band-aid approach to systems development which invariably leads to higher costs in the long run. These higher costs are the result of "throwing good money after bad" in a series of interim fixes which delay the recognition of a system's inadequacy, but do not prevent its inevitable obsolescence. As a result, many organizations end up spending more than would have been necessary if technical architecture planning had been made from an appropriate sunk cost perspective.

4. Resources.

Scarce, shrinking personnel and dollar resources significantly constrain the planning and implementation of transition architectures. Immediate needs are often so pressing that available resources are committed in stop-gap, interim measures as described above. This crisis management is symptomatic of inadequate technical planning which has failed to influence the formal resource allocation/budgeting process (POM, PPBS). It is a self-perpetuating failure which results when planning staffs become focused on interim solutions and thereby neglect the adequate forecasting and justification of future requirements. This in turn perpetuates the problem. Obviously, breaking this

cycle is a critical step in developing an effective technical architecture. Planners must avoid the pitfalls of the temporarily urgent and work instead to ensure adequate resources are forecast and programmed to meet future needs.

5. Technology.

Changing technology complicates the task of technical architecture planning. On one hand, building a technical architecture solely around existing, proven technology allows decision makers to know the exact capabilities of planned systems. Yet, ignoring technological advances may result in an organization's systems becoming obsolete even before they are fully operational. Obsolescence means less available support and inevitably leads to higher maintenance and operations costs. On the other hand, embracing the newest technologies also involves risk. Planning technical architectures around unproven technologies can lead to large expenditures and results which don't meet expectations. The challenge decision makers face is to strike an appropriate balance between proven and emerging technologies to plan and procure flexible systems whose price-performance ratio will remain favorable well into the future.

Developing technical architectures which take advantage of new technologies while minimizing risk is often an unavoidably subjective task requiring predictions about future systems requirements and technological trends. An organization must take a proactive approach to evaluating new technologies. Its planners must work to stay abreast of current developments

and trends through the careful study of professional journals, participation in expert conferences, and internal research. Although it is not possible to fully eliminate the risks associated with new technologies, they may be reduced to a manageable level through careful study and the use of formalized methods for evaluating emerging technologies. Trends in the private sector and government standardization guidelines are a good source of direction in selecting and evaluating new technologies.

6. Standards and Guidance.

Following established standards is not only mandatory in planning technical architectures, it is also highly advisable. Government standards and formal directives are designed to help avoid some of the pitfalls mentioned above. By carefully designing technical architectures to adhere to standardization guidelines, an organization guarantees maximum interoperability among systems and recognizes additional benefits, such as system flexibility and vendor independence. Several guidelines are significant in studying NMPC's internetwork connectivity requirements. The CNP CIRMP and the CNP TAP have been discussed as important sources of guidance and direction for NMPC's technical planners. Additionally, they are constrained by several other important standards including the Government Open Systems Interconnection Profile (GOSIP). Appendix E provides a discussion of its provisions. GOSIP is a subset of the International Standards Organization's Open Systems Interconnection Model (ISO OSI) -- the preeminent international framework for

internetwork connectivity (See Appendix C). Additionally, NMPC's planners must consider IEEE standards (Appendix D), and various DOD and DON instructions in developing appropriate technical architectures. These standards and guidelines play an important role in defining NMPC internetwork connectivity alternatives as discussed later in this study.

E. THE CNP TAP AND NMPC'S TECHNICAL ARCHITECTURE.

The CNP TAP addresses baseline, transition, and target technical architectures for NMPC and all elements of the CNP claimancy. It highlights some common problems in technical architecture planning and asserts that current baseline architectures demonstrate several weaknesses. Primarily, there has been a lack of adherence to standards, architecture decisions have "generally been made after the fact . . . to conform to the existing environment rather than through advanced planning", and that hardware/software selection decisions have been inappropriately driven by external factors. [Ref. 4:p. 39] This appears to have led to a fragmented approach to systems development in which the rise of end-user computing and trends toward distributed data processing have been inadequately orchestrated. The results are departmental systems which either do not effectively share data or cannot interact as necessary to support the overall goals of the CNP Claimancy.

Although the CNP TAP well defines transition and target technical architectures in broad terms, it does not adequately address the details of

management and implementation of planned systems. It is meant to be a broad, conceptual documentation of the CNP Claimancy's technical architecture -- a purpose it serves extremely well. It is not meant to provide the details of implementation within each organization of the CNP structure. This is a task appropriately left to the organizations themselves working within its broad guidelines -- hence the purpose of studies such as this one.

F. THE CNP TAP AND CNP CIRMP IN NMPC INTERNET DEVELOPMENT.

Both the CNP TAP and CNP CIRMP portray a target information systems environment for NMPC in which a multitude of local area networks are interconnected to form an effective, organization-wide internet. The ultimate goal is to interconnect departmental networks allowing access to mainframe resources and Navy MPT wide area nets in order to achieve effective resource sharing and distributed processing in support of corporate systems while fostering departmental end-user computing initiatives. To be successful in constructing such a comprehensive internet will require careful planning and development. The continuing procurement and installation of office area networks must be managed with an eye toward facilitating internetwork connectivity while making the best possible use of limited funding and organizational resources. The next four chapters examine the functional requirements of an NMPC internet, introduce the systems to be connected, and explore the technical feasibility of alternatives for doing so.

V. INTERNET FUNCTIONALITY REQUIREMENTS

A. INTRODUCTION.

In studying NMPC's present and planned information systems, a clear requirement for an organization-wide internet emerges. The initiatives outlined in the CNP CIRMP and the technical architectures discussed in the CNP TAP imply that there is a growing need to interconnect departmental office area networks and NMPC mini and mainframe based systems. This chapter discusses the functional requirements of NMPC's departmental nets and the corresponding requirements of a comprehensive internet.

B. FUNCTIONAL REQUIREMENTS OF DEPARTMENTAL OAN'S.

Recalling from Chapter 3, the CNP CIRMP specifies an IRM environment built upon initiatives fostering greater end-user computing, developing effective organization-wide databases with increased distributed data processing, and facilitating the sharing of data and resources across departmental lines. Local area networks are well suited to these goals. Numerous LAN's/OAN's have been installed throughout NMPC and many more are planned for installation. Clearly, they will continue to proliferate as NMPC strives to meet the stated and implied goals of the CNP CIRMP and TAP.

Adequately identifying functional requirements is key to managing this growth of networked computing and essential to designing effective technical solutions to meet business needs. Under NMPC's current approach to network planning, the identification of functional requirements is left largely to the network users. A department identifies a need for a LAN, outlines the functions to be performed, and submits a request for its procurement and installation via NMPC-163, the Customer Support Division. NMPC-163 assists in translating the request into a workable network design and prepares Abbreviated System Decision Papers (ASDP) and other documents necessary to begin the acquisition process. Once approved, NMPC-163 assists in managing the installation of the network and provides for necessary personnel training to complete its implementation. The functional requirements identified and discussed below were determined by interviewing key personnel from NMPC-163 and studying the network ASDP's available from their files. Appendix H lists the functional requirements of each departmental LAN. It shows universal requirements for word processing, spreadsheets, database management and business graphics among the departmental networks. Recognizing this, NMPC has adopted standard LAN versions of PC software applications to meet these requirements.[3] By encouraging the use of common standard software (WordPerfect, DBASE,

[3]The CNP CIRMP discusses this move toward standard LAN versions of applic tions software for word processing, database management, spreadsheets, and business graphics but also allows the purchase of non-standard, specialized software when requirements call for it. [Ref. 1:p. 7-4]

Lotus 1-2-3, etc), training requirements are reduced and the exchange of data between departments is greatly facilitated.

Some of the departments require other specialized microcomputer applications such as those for project tracking and desk top publishing. Although these specialized packages are not found in all departments, their impact on network functional requirements is not significantly different from that of the standardized packages. Specifically, data storage and backup, file sharing, locking, access control and related functions to ensure data integrity are the basic functional requirements associated with these applications. The files they produce and manipulate are among the data to be exchanged between departments. Thus, file management and transfer is a basic functional requirement to be met once departmental LAN's are internetworked.

In reviewing each department's LAN justifications, E-mail was listed as a requirement by most, but not all of them. Of those listing this requirement, some indicated a need for E-mail solely internal to their department while others listed requirements for both intra- and interdepartmental E-mail capabilities. Although some departments did not list a need for E-mail, interviews with NMPC-16 personnel indicated that the senior NMPC leadership envisions the need for a universal E-mail capability. Obviously, internet E-mail is an additional functional requirement to be met.

The next significant requirement found for several of the departmental LAN's was a need for mainframe access to accomplish file transfer and for

terminal emulation to access and run both mini and mainframe applications on NMPC processors. Additionally, several departments indicated a need for modems and communications software in order to access remote processors in other government organizations. This need to access and run remote programs applies only to those systems based on mini and mainframe applications. There does not appear to be any requirement to access microcomputer applications residing on other departmental LAN's.

In addition to these functional requirements, each departmental LAN will require network management, maintenance, and tracking functions. File, print, and communications server software must provide for effective network utilization. Security controls to prevent unauthorized access to data and equipment are also important functional considerations and will be complicated further by internetwork connectivity.

C. INTERNET FUNCTIONAL REQUIREMENTS.

As implied above, the formation of a comprehensive NMPC internet by interconnecting its independent departmental LAN's and mini/mainframe systems will require the following functional requirements: file management and transfer, E-mail, terminal emulation, communications access to remote processors, security functions, and network management utilities.

Hardware and software to accomplish internet connectivity will need sophisticated addressing, routing, and protocol conversion capabilities. Network

management, maintenance, and diagnostic functions will be complex; yet essential to reliable network operations. Security challenges will be compounded for there is a greater need for access controls as resource sharing extends beyond departmental lines.

Achieving these internet functional requirements is far from a trivial task and requires advanced hardware and software technical solutions. Connecting LAN's to form an internet is not simply a matter of splicing cable. Accomplishing internetwork connectivity requires the use of specialized devices, primarily bridges and gateways. The first step in identifying the specific connectivity devices necessary to build and NMPC internet is to identify the LAN's and resource to be connected. Accordingly, this is the subject of the next chapter.

VI. NMPC NETWORKS AND RESOURCES

A. INTRODUCTION.

Existing systems and resources are the logical starting point for designing transition and target technical architectures which will meet NMPC's goal of a comprehensive, organization-wide internet. NMPC's existing and planned information systems resources are depicted in Figure 5 and discussed below.

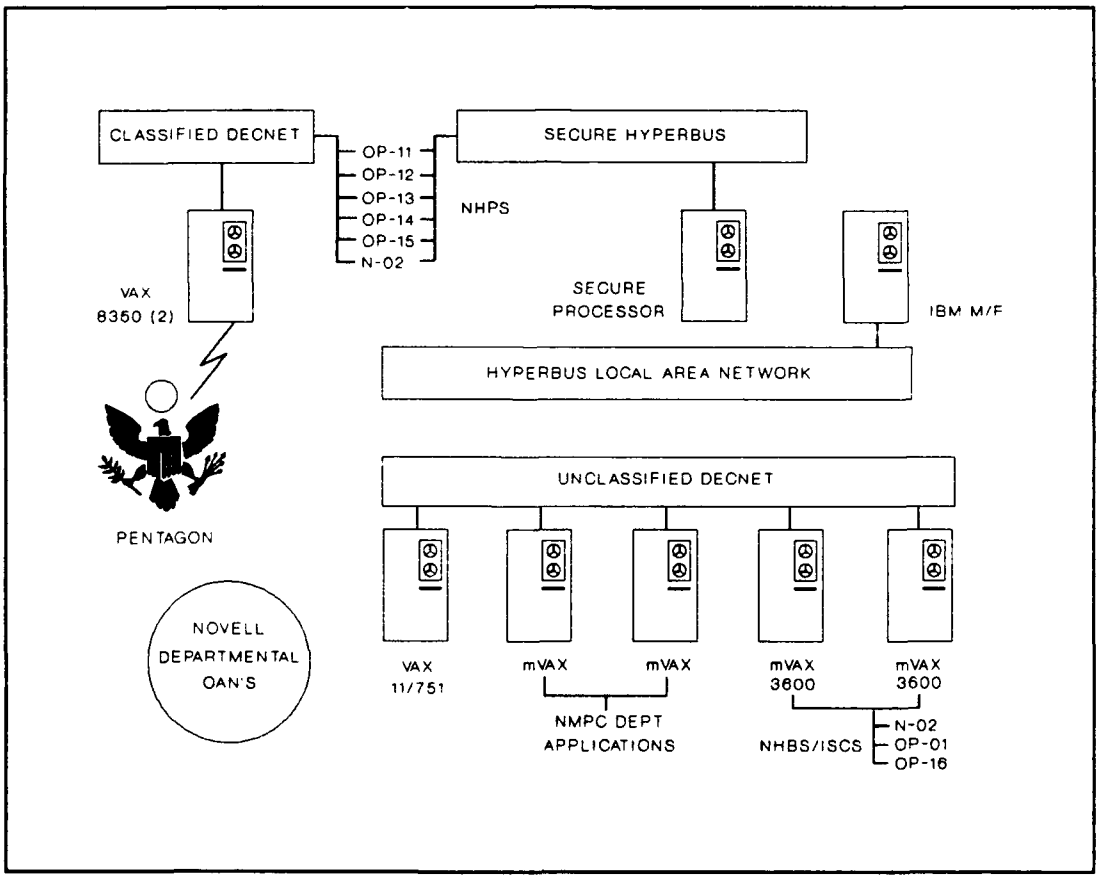


Figure 5: NMPC's Baseline Systems

B. EVOLUTION OF NMPC'S BASELINE ARCHITECTURE.

NMPC's current computer and communications infrastructure (baseline architecture) is typical of most large government or corporate organizations. It consists of various mainframe, mini, and microcomputer systems which for the most part function independently of one another. The rapidly changing technologies of the 1970's and 1980's led to an equally rapid expansion in their operational application in large organizations. As information systems grew beyond centralized transaction processing to support all facets of business operations, the evolutionary pace of development often exceeded the capacity of organizations to manage its growth. As a result, NMPC, like many large organizations, finds itself with large resource investments in various information systems which do not yet work together as effectively as desired.

NMPC relies heavily on its computing resources to perform day-to-day business operations. This reliance is growing steadily with the proliferation of microcomputers, office area networks, and the expansion of distributed data processing and end-user computing throughout the command. Recognizing the need to incorporate these systems into a coherent organization-wide information management system, NMPC sees it is now necessary to develop specific plans for doing so. Networking and internetwork connectivity are critical parts of such plans. An understanding of existing systems is the starting point for defining these requirements.

C. IBM MAINFRAMES.

NMPC's mainframe resources are consolidated in the NMPC Headquarters Data Processing Center located in the Arlington Navy Annex. They provide processing for NMPC's internal applications as well as offering remote support to the Navy's Consolidated Data Center (CDC) located in Bratenahl, Ohio via a Navy Manpower, Personnel, and Training wide area network. Through this net, NMPC serves as the Remote Input/Output Center (RIOC) and Associated Data Processing Center (ADPC) for the CDC.

There are six major IBM processors currently in use by NMPC: one IBM 3033, three IBM 4381's, and two IBM 4341's. The IBM 3033 is NMPC's principal unclassified processor serving approximately 500 local terminals, 306 PC's and 93 printers through the HYPERbus local area network (discussed below). The three IBM 4381's are processors dedicated to the Naval Military Personnel Distribution System (NMPDS) administered by NMPC-47 and serve approximately 764 local terminals and 68 printers also on the HYPERbus network. The two IBM 4341's are NMPC's principal classified processors serving secure DTE's and other devices through a separate, classified HYPERbus network.

D. HYPERBUS LAN.

The backbone of NMPC's existing telecommunications infrastructure is an early type of local area network produced by Network Systems Corporation (NSC) called a HYPERbus. Table 1 summarizes the technical specifications of a

HYPERbus LAN. Readers who are unfamiliar with the distinguishing characteristics of local area networks (LAN's) will find it useful to refer to Appendix B for a general discussion of the characteristics of LAN's.

Table 1: Summary of HYPERbus Specifications

HYPERbus SPECIFICATIONS	
Transmission Technique:	Baseband
Topology:	Multiple Linear Bus
Access Method:	CSMA/CA
Maximum Data Rate:	10M bps
Maximum Transmission Distance:	4,000 feet
Transmission Medium Supported:	75 ohm broadband Coaxial Cable
IEEE 802 Standards Supported:	None
High-Level Protocols Supported:	None
Maximum # of Devices Supported:	128 per cable segment
End-User Devices Supported:	Minis, IBM PC's & compatibles, ASCII & 3270-type terminals
Vendor-Supplied Devices:	Network interface with adapter card
Vendor-supplied Software:	NOS, utilities & applications

The HYPERbus LAN is the backbone of NMPC's primary unclassified network. Its current configuration connects 1,228 terminals, 161 printers, and

306 PC's in a network which allows users to access NMPC's IBM mainframes.[4] The HYPERbus LAN uses baseband transmission over 75 ohm coaxial cables with a maximum data rate of 10M bits per second. It has a bus topology consisting of a central backbone connecting four branch buses. Bus Interface Units (BIU's) dispersed throughout the building are used to tie devices into the network. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is the access method by which the net is governed. The primary functions performed by the net include IBM terminal and PC connectivity to allow micro-mainframe file transfer.

Although the HYPERbus appears capable of supporting further expansion through the addition of new devices, it suffers from a major drawback in that it does not conform to current industry and government network standardization guidelines. This limitation is a significant potential obstacle to effective internetwork connectivity which will become more critical as the number of diverse nets within NMPC increases. NMPC already has many networks in use and is in the process of installing others throughout the organization. These are primarily DECnet and Novell networks as discussed below.

[4]The devices connected to the Hyperbus fall into two categories: those of NMPC in general and those dedicated to use by NMPC-47 in its role as administrator of the Naval Military Personnel Distribution System (NMPDS). NMPC's devices: 464 terminals, 93 printers, and 306 PC's. NMPC-47's devices: 764 terminals and 68 printers.

E. DEC NETWORKS.

NMPC has various DEC equipment and networks in place or projected for installation in the near term. An exact forecast of which systems will be fully installed by what point in time is not possible due to on-going vendor protests delaying implementation of current contracts.[5] Nevertheless, it is possible to examine the expected technical architectures and how they affect NMPC's goal of a comprehensive, organization-wide internet.

The Navy Headquarters Budgeting System (NHBS)/Navy Headquarters Programming System (NHPS) are systems which have already been funded and substantially implemented. These are not solely NMPC-specific systems, however, their use will be heavily influenced by NMPC's requirements. The NHPS portion of the system involves classified data and is built around two VAX 8350 processors located at the Pentagon. Since it is a classified net, NHPS is not discussed at length herein. For the purposes of this study, it is sufficient to understand that NMPC users access the classified DECnet which supports NHPS through the use of dial-up access over secure lines and cryptologic communications devices. The NHBS on the other hand is an unclassified system whose components are to be located at NMPC. The heart of the NHBS system

[5]For example, a DECnet backbone planned for full implementation in FY 89 has been indefinitely delayed by a vendor protest. This net was to be a key element of NMPC-163's plan for an overall NMPC internet. If a different net is installed as a result of the protest, it could significantly complicate interconnectivity requirements.

is two microVax 3600 processors used primarily by NMPC-02, OP-01, and OP-16.[6] As fully implemented, users will access NHBS over a standard DECnet.

DECnet is the transparent network software NMPC uses on its standard Ethernet LAN's, such as in support of the NHBS system. It allows any node in the LAN to initiate and participate in terminal-to-terminal, program-to-program, or task-to-task communications with other nodes [Ref 5.]. The LAN consists of a bus topology with a peer relationship between nodes. It uses a baseband transmission medium (10Base2) in the form of ThinWire Ethernet coaxial cable set up in a dual cable system to allow full duplex communications. It uses digital, phase-encoded transmissions and can support a data rate of up to 10M bps. Transmissions across the net are broadcast to all stations. The net uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) for medium access control and conforms to IEEE 802.3 standards. Nodes are connected to the net using Digital Equipment Corporation (DEC) communications controllers and clamping mechanisms that allow nodes to be added to or removed from the net without disrupting it.

In addition to the DEC equipment which makes up the NHBS system, NMPC anticipates the potential addition of one, possibly two microVax systems to support related departmental applications. These may be built around microVax 8210's, but the exact nature of the systems if approved, has not yet been

[6]Refer to Chapter 1 for an understanding of the dual role of NMPC organizations as OPNAV organizations.

finalized. Although their exact components have not been determined, it appears that they will be implemented through the use of a thin ethernet.

Ultimately, NMPC plans that these systems, the NHBS, and an existing VAX 11/751 will be tied together by the addition of a thick Ethernet backbone. This backbone was originally scheduled for installation in FY 1989 but has been delayed indefinitely due to a vendor protest of the contract. Additionally, a series of office area networks (OAN's) currently in various stages of implementation are also to be tied into this ethernet backbone. These OAN's are primarily Novell networks and are briefly described below.

F. NOVELL NETWORKS.

In response to advances in computer technology and in compliance with the IRM strategy of the CNP CIRMP, NMPC is undergoing a rapid increase in departmental end-user computing and an expanded use of distributed databases and data processing. A significant result is the proliferation of office area networks within NMPC. There are as many as two dozen such networks either fully implemented or presently in some stage of contracting or installation. Their size ranges from approximately a half dozen to as many as eighty terminals/PC's on each net. Appendix G gives a more specific summary of these nets.

NMPC uses various versions of Novell Netware, a fully distributed, multitasking operating system to run these nets. Novell provides excellent

handling of I/O intensive operations and manages simultaneous requests for resources effectively [Ref. 6]. The LAN's are built on a logical bus topology and support primarily PC's (Zenith 248's), various printers, and some terminals. In general, these nets use single channel transmissions across baseband coaxial cable and can support a data rate of up to 10M bps. They are governed with a CSMA/CD method of medium access control and conform to IEEE 802.3 Ethernet standards.

G. THE MAPTIS GRID.

The Manpower Personnel and Training System (MAPTIS) Grid is a communications grid located in NMPC's facilities at the Arlington Naval Annex. It is an older system installed to provide connections for terminals and other I/O devices throughout NMPC to its IBM mainframes through front-end processors. Interviews with NMPC-167 personnel indicate that although the system remains in use to a limited degree, it is no longer actively maintained [Ref. 7]. As portions of it fail, they are not restored. Nevertheless, it is a communications structure which remains in place and is worthy of brief discussion.

The grid consists of several hundred twisted-pair, point-to-point links run throughout the building. Data Termination Equipment (DTE) is connected to given lines through the use of a modem. Each line terminates on a panel of a selected front-end processor within the central computer room and through it is connected to the appropriate IBM mainframe. Switching between processors is

done manually by changing the panel on which a given line terminates. The grid is therefore limited in switching flexibility as its point-to-point links are fixed and require manual switching to access different processors. Additionally, the grid is limited by its twisted-pair transmission media. In general, twisted-pair is susceptible to interference and noise. The grid is no exception. According to a technical study, interference and lost data is a common problem for those DTE's still using the grid [Ref. 8:p. 19].

Unpredictable reliability is another significant limitation of the grid. Since there is no evaluation and maintenance program for the grid, there is no data available on how many of its lines are functional. When devices are connected to the grid, a trial and error method must be used to find working lines. This is done by connecting a DTE to a wire and connecting the other end of the wire, if locatable, to a panel in the computer room. If it works, the line is used. If not, alternative lines are tried. [Ref. 8:p. 19] Although the grid allows distribution of terminals where working lines may be found, its potential for further use appears severely limited without a significant investment in a technical evaluation and maintenance program to detect and correct problems in the grid.[7] Although the MAPTIS grid has some limited potential for use, it does not appear suited for use as part of a comprehensive solution to NMPC's internet needs.

[7]The current state of the MAPTIS grid and its potential for further use may perhaps be best summarized in comments made by CDR Carpenter, Chief of NMPC-1633 who described it during an interview on 26 September 1989 as "completely unmanageable" given its neglected state.

H. A COMPREHENSIVE NMPC INTERNET.

NMPC is seeking to incorporate the systems/resources described above into a comprehensive, organization-wide internet in order to allow information sharing across departmental and system boundaries in support of corporate information systems initiatives. The concept is solid and well supported by NMPC's business requirements; however, selecting an appropriate internet architecture requires first determining the feasibility of connecting NMPC's diverse systems and then selecting the most appropriate devices for doing so.

In simple terms, NMPC's internet goal is to tie together its Novell OAN's and DECnet systems in a manner which provides access to the command's IBM mainframes and yet preserves the capabilities now embodied in the HYPERbus network. Our study implies a series of connectivity requirements which might be used in building internet alternatives. Specifically, the feasibility of achieving the following six system-to-system connectivity configurations should be considered in determining potential internet designs:

- HYPERbus - Novell
- HYPERbus - DECnet
- Classified HYPERbus - Classified DECnet
- DECnet - IBM
- DECnet - Novell
- Unclassified DECnet - Classified DECnet

Figure 6 shows these potential system-to-system connections. Obviously, implementing all of these connections would result in needless duplications and in some cases conflict. More practical solutions may be found by building an internet using some subset of the possible connections shown here.

To design an effective internet, each connection must first be evaluated for its technical feasibility and practicality in the NMPC environment. Those connections which prove feasible may then be used as building blocks to design alternative internet configurations suited to NMPC's requirements. These issues are addressed in the following two chapters.

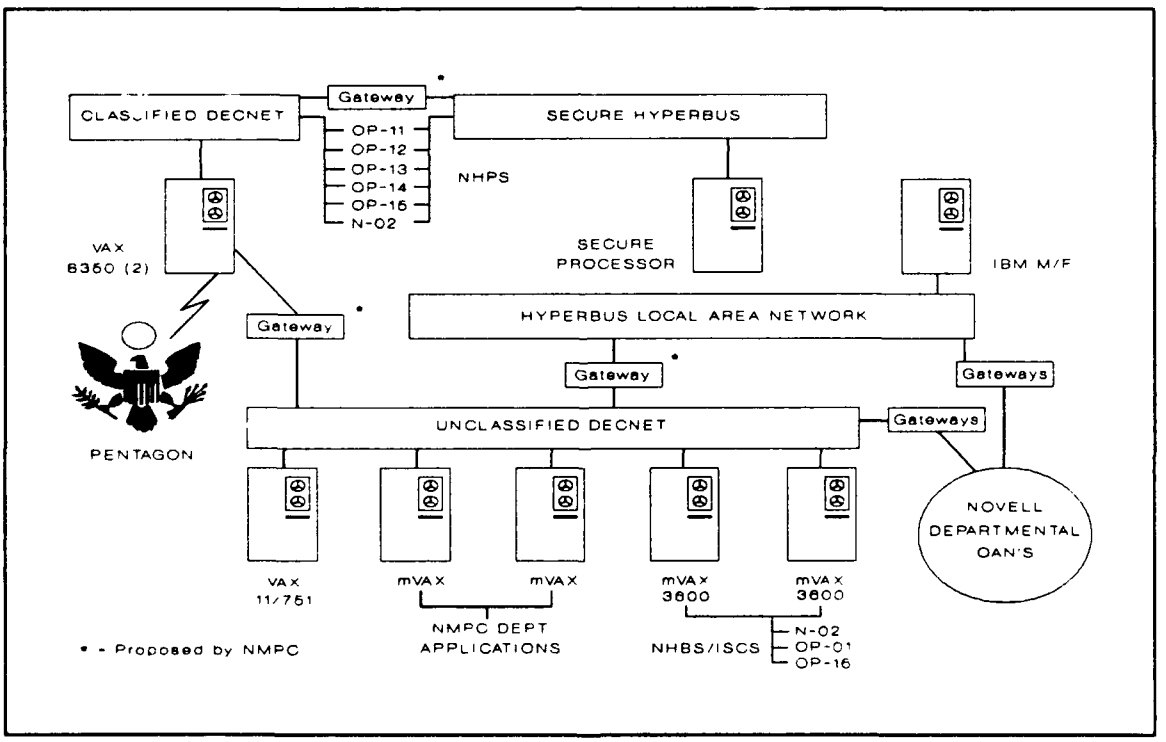


Figure 6: Potential NMPC System-to-System Connections

VII. POTENTIAL GATEWAYS AND BRIDGES FOR AN NMPC INTERNET

A. INTRODUCTION.

This chapter discusses the technical considerations and practicality of the system-to-system connections which might be used in building an NMPC internet. It is written with the assumption that the reader is familiar with the characteristics of bridges and gateways -- the two most common devices used to connect local area networks. Readers who are unfamiliar with these devices should read Appendix F before continuing. Similarly, Appendix G provides a discussion of the DEC, Novell, and HYPERbus network architectures upon which much of this chapter is based.

B. HYPERBUS CONNECTIVITY.

The HYPERbus represents a significant existing resource providing mainframe access to approximately 1600 terminals and PC's and access to approximately 150 printers [Ref. 4]. The coaxial cable connecting its devices extends throughout the Navy Annex. The opportunity to make use of this existing infrastructure and avoid the need to run additional cable makes its use as part of an internet solution particularly attractive. It is possible to connect individual terminals or PC's to the HYPERbus by using adapter cards in

conjunction with various BIU types (Appendix G); however, accomplishing LAN interconnectivity is a far more complex problem [Ref. 9].

The HYPERbus is older technology which does not comply with any OSI, GOSIP, or IEEE standards [Ref. 10]. It is a connection-oriented, virtual circuit network whereas the DEC and Novell networks are in effect connectionless, unreliable datagram networks. Internetworking connectionless and connection oriented networks together to form an internet is an extremely difficult technical challenge which may not in fact be possible. Tanenbaum presents an excellent description of the difficulties associated with attempting such interconnectivity. In discussing internets built using a virtual circuit network, he concludes "It [an internet built with gateways] has the disadvantage of being difficult, in not impossible, to implement if one of the networks involved is an unreliable datagram network [Ref. 11:p. 346]." He further states that when connectionless networks (e.g. DEC, Novell) are involved ". . . serious problems occur if the internetworking strategy is based on virtual circuits." (e.g. HYPERbus) [Ref. 11:p. 346].[8]

Thus, it is reasonable to conclude that building an NMPC internet around the HYPERbus may not be feasible and if attempted will require a complex, customized hardware and software solution. Nevertheless, there is considerable NMPC interest in using the HYPERbus as part of its internet. Therefore, the

[8]The specified examples (e.g. . . .) have been added for clarity in this discussion and were not specifically cited by Tanenbaum.

following discussion outlines some of the obstacles which gateways to the HYPERbus would have to overcome.

1. HYPERbus - Novell Gateway.

In discussing the characteristics required of a gateway to connect a Novell LAN with the HYPERbus, it is first important to understand the significant differences that exist between these networks. Once these differences have been described a conceptual design of the gateway will be presented.

a. Comparison of HYPERbus and Novell Network Architectures.

This discussion highlights the most significant differences between the Novell and HYPERbus network architectures. A more complete description of each architecture is presented in Appendix G and may serve as a reference for the information presented here.

(1) Transmission Media and Traffic Capacity. The HYPERbus uses a 75 ohm, coaxial cable and baseband signaling supporting a data rate of up to 10M bps; whereas, NMPC's Novell nets use a 50 ohm coax cable, baseband signaling and a maximum data rate of 10M bps [Ref. 12, Ref. 6]. Therefore, the gateway design will require signaling and attachment hardware compatible with each of these different mediums. It should be noted that the HYPERbus' 75 ohm cable has the drawback of experiencing more signal attenuation over distance and hence greater susceptibility to noise than does the 50 ohm cable

used in the Novell nets; however, this should not affect the gateway design significantly.

In terms of data rate, both nets offer similar traffic capacities sufficient to handle the rates necessary to support NMPC's functional requirements. Data transmission rates vary by data type and device supported. NMPC's requirements for processing text files on network devices ranging from printers and plotters (300 - 20K bps) to storage devices and terminals (.25M - 10M bps) can easily be supported by both networks' transmission media. [Ref. 13]. When networks connected across a gateway differ in maximum data rate, it is necessary to build buffers into the gateway in order to prevent one network's transmissions from exceeding the other's data capacity. Since both the HYPERbus and Novell networks support the same maximum data rate, transmission buffering will not be a significant requirement in the gateway design.

Nevertheless, there is a potential traffic capacity problem associated with connecting the Novell networks to the HYPERbus. Reviewing the LAN functionality chart in Appendix H shows that less than one third of the departmental LAN's require mainframe access, but virtually all of them will require interdepartmental access across the internet. The HYPERbus is presently used primarily for terminal access to the IBM mainframes. The addition of a great deal of interdepartmental traffic across the HYPERbus may adversely effect response times for the terminals. The extent of this

performance degradation may only be determined by a technical study, simulation, and testing. Because the potential for performance degradation exists, conducting such a study is essential attempting to form an internet using the HYPERbus. It is a cost which must be considered in evaluating the feasibility of building Novell-HYPERbus gateways.

(2) Topology. Both the HYPERbus and Novell LAN's use a bus topology. Implementing gateways to connect each Novell LAN to the HYPERbus will exceed neither the permissible bus segment lengths nor the number of hierarchical segments feasible within a single network. This does not mean that topology considerations may be ignored in the gateway design. The HYPERbus uses special bus interface units (BIU's) to accomplish connection between network bus segments (Appendix G). These BIU's are intelligent devices which must be programmed with specific information about network topology and updated whenever the topology changes. Since the BIU's perform addressing and routing functions the gateway design will have to assume these functions. The addition of over two dozen Novell nets and the hundreds of devices they support will increase the frequency of network changes, and hence the reprogramming of BIU's (or gateways acting as BIU's) necessary to keep the internet functioning effectively. This additional manual maintenance requirement is a drawback of using the HYPERbus as a backbone for connecting the Novell networks. [Ref. 12]

(3) Medium Access Control Methods. The HYPERbus medium access control method does not comply with any IEEE standard [Datapro]. It uses a specialized CSMA method that its Systems Description Manual describes as a "virtual token passing scheme which provides predictable response times and maintains stability at high loads" [Ref. 12:p. 1-1]. The HYPERbus' unusual contention method allows individual BIU's to be programmed with one of three transmission priorities. This means that they do not contend for network access on a peer basis as is the case under most contention schemes. [Ref. 12]

This differs significantly from the Novell networks' CSMA/CD access method which meets IEEE 802.3 standards [Ref. 6]. Resolving these differences in medium access control will be a significant challenge for the gateway to meet. The gateway must be designed to duplicate and replace the functions of the BIU in order to achieve access to the HYPERbus. Since the HYPERbus treats every BIU distinctly and each BIU can be programmed with only one transmission priority, it is likely that a gateway performing BIU functions would have the same limitation [Ref. 12]. In effect, each Novell network would take on a single priority for all its devices' transmissions. This presents a severe network management problem in that not all devices on a Novell net may warrant the same priority. For example, a Novell net with many devices needing only routine access and a few devices requiring high priority access could only be assigned a single priority. In such a case, a high priority access could be assigned to the net. If the net's low priority devices produce high

traffic volume they might inappropriately dominate the internet since all of their transmissions would receive a high priority across the gateway. This is certainly a drawback of gatewaying the Novell nets to the HYPERbus.

b. Frame Formats, Addressing, and Routing.

Although differences in transmission media, topology, and access method are significant gateway considerations; reconciling the differences between frame formats, addressing, and routing functions is a far more challenging aspect of connecting the HYPERbus and Novell networks. The HYPERbus was not designed to accommodate connections with diverse nets.[9] Unlike the Novell networks, it does not adhere to open systems standards. Although there are some specialized commercial products which will allow limited HYPERbus access by an individual terminal or PC, there are no pure gateways available. Building a fully functional gateway between these systems will therefore require carefully selected hardware and complex, custom-designed software. Although it may be possible to develop such software, the feasibility of doing so successfully is quite questionable.

(1) Frame Formats. Figure 7 on the next page shows the frame format of the HYPERbus and Novell networks. On the HYPERbus, data is encapsulated in frames by the BIU and transmitted across the net. Each of these frames consists of a header containing routing and priority information,

[9]The HYPERbus was designed to support full connectivity only with a companion NSC system called HYPERchannel. [Ref. 12]

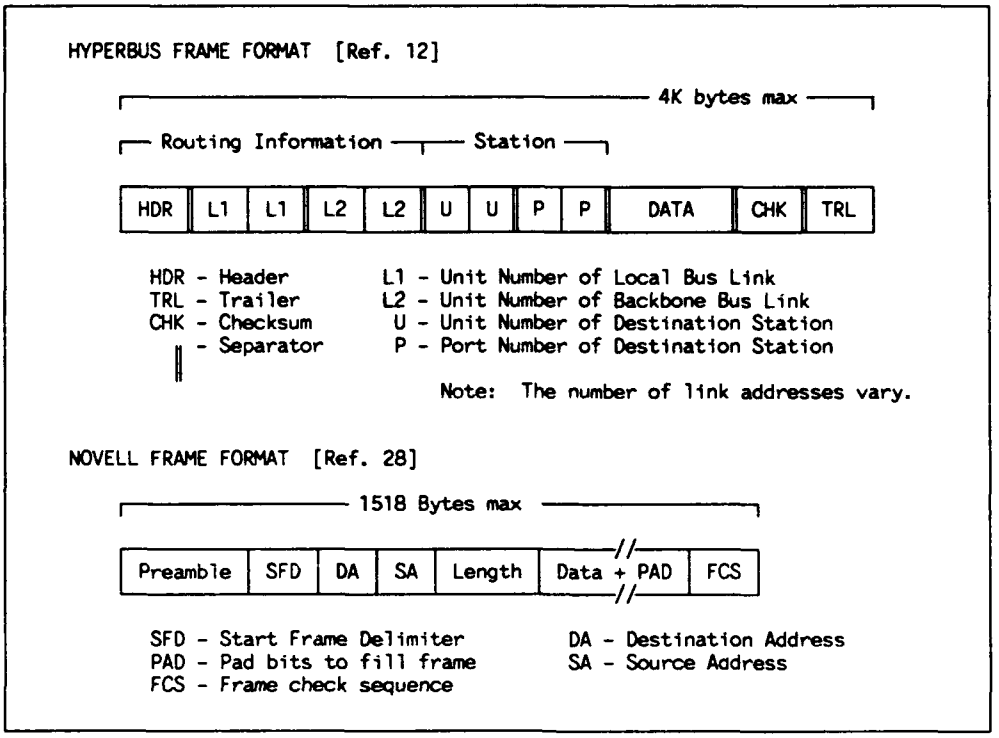


Figure 7: Comparison of HYPERbus and Novell Formats

a 16-bit cyclic checkword, and a body of data which together may form a frame of up to 4K bytes in length [Ref.12]. The Novell frame format is significantly different using a standard 802.3 ethernet format consisting of a preamble, a start frame delimiter, destination address, source address, data length field, the data itself, a pad field (used to ensure all frames meet a minimum 64 byte length), and a 32-bit checksum which together may not exceed a maximum length of 1518 bytes. [Ref. 11:p. 145, Ref. 14:p. 119]

Since the maximum frame sizes differ between the networks (4K bytes HYPERbus vs. 1.5K bytes Novell), the gateway will be required to accomplish frame fragmentation. Each incoming HYPERbus frame will need to

be reduced into several Novell network frames. The additional processing associated with this task will require a significant buffering capacity in the gateway (which as mentioned above would not be required for data rate considerations alone). Performing this fragmentation function leads to another design consideration: whether or not frame reassembly should be built into the gateway so that smaller Novell frames might be reassembled into fewer larger frames before being transmitted to their HYPERbus destinations. If the gateway does not perform reassembly functions, then it would be left for the destination stations to do so. As a result, transmissions coming onto the HYPERbus from the Novell networks would consist of a far greater number of smaller than optimal frames. This would increase the amount of overhead data (headers, addresses, etc.) in proportion to the data being transmitted. Thus, traffic volume on the HYPERbus would increase disproportionately and result in reduced efficiency and performance. This could be avoided by building reassembly functions into the gateway; however, doing so would slow its processing considerably. This would further increase the need for buffering and the potential for the gateway to be overwhelmed by incoming traffic.

(2) Address and Routing Considerations. Reconciling frame size differences is less challenging than the need to perform the conversion of address and routing characteristics between the networks. Herein lies the most significant obstacle to constructing an effective HYPERbus-Novell gateway. The way in which each network performs addressing and routing functions

differs significantly. HYPERbus is a connection-oriented, virtual circuit network and Novell is a connectionless, datagram network [Ref. 12, Ref. 14]. The technical feasibility of constructing a gateway is questionable and it is very unlikely that it can be done effectively. Nevertheless, if attempted, a HYPERbus-Novell gateway design would have to resolve addressing and routing differences as discussed below.

On each Novell network, addressing is very straightforward. The 802.3 CSMA/CD frame format provides for the use of either 16-bit local addresses or 48-bit global addresses [Ref. 11:p. 145]. In an internet configuration consisting of solely 802.3 networks, routing is greatly simplified by using connectionless gateways and the 48-bit global addresses. Such addresses are unique for each existing ethernet node worldwide.[10] Thus, when dealing solely with 802.3 compliant networks it is a simple matter to compare a frame's global address to a routing table within the gateway and forward it accordingly. Unfortunately, HYPERbus works on a connection-oriented basis and its addressing and forwarding functions are therefore quite different and incompatible with those of the Novell networks [Ref. 12].

HYPERbus addressing is accomplished through a hierarchical scheme corresponding to the topological structure of the net. Each station on the net has a unique physical address. In routing a transmission, a full network

[10]These global addresses are assigned by the IEEE to ensure that each ethernet node throughout the world has a unique address, with a total of 7×10^{13} possible worldwide [Ref. 11:p. 145]. They are established at the time of manufacture with each ethernet adapter card having a unique, built-in address.

address is assigned which consists of the station and unit numbers of all link BIU's lying between the origin and destination stations. Transmissions on the network are accomplished through the establishment of a virtual circuit. A terminal dials a connect request that must contain the addresses of all BIU's along the desired path. Normally, the user must provide this path through a dialing function in which he provides the BIU addresses of all intervening link BIU's with the destination address. Clearly, in an internet as large as that proposed for NMPC this manual process would not be feasible. Although HYPERbus supports an alternative (logical dialing) in which the user must only supply a destination name, it is only available when the network includes a Bus Service Center (BSC). [Ref. 12]

Since it is neither practical nor technically feasible to install a BSC on each Novell network, the gateway itself must be designed to provide the logical dialing function. This introduces another design complication. The HYPERbus does not support adaptive routing to accommodate network changes. Instead, it relies on fixed routing and manual updating of a BSC's routing information. For this reason, even if a gateway can be designed to perform the BSC's logical dialing functions, changes to the net could require the manual updating of each Novell-HYPERbus gateway. This represents an extreme network management problem which suggests that an internet built using such gateways would be difficult to manage effectively.

b. HYPERbus-Novell Gateway Considerations Summarized.

The comparison of the HYPERbus and Novell network architectures presented above suggests the following would be required in a gateway connecting them:

- Connection to and signaling across 50 and 75 ohm coaxial cable.
- Ability to buffer and perform segmentation/reassembly functions of transmission frames.
- Overcoming the challenges of internetworking connectionless networks with a connection-oriented network by providing some means of accomplishing conversion of frame formats and addressing and the ability to perform vastly different routing functions on each side of the gateway.

Additionally, since the HYPERbus and Novell networks differ entirely, the gateway would also be required to perform a variety of functions to accommodate incompatible error checking and recovery schemes, differing timeouts, and dissimilar status reporting mechanisms. Clearly, the specific design of such a gateway is a complex task and beyond the scope of this study.

2. HYPERbus-DECnet Gateways.

Using the HYPERbus as part of a comprehensive NMPC internet would also require building gateways to connect NMPC DECnets (e.g. NHBS and the planned DECnet backbone). This is a problem very similar to that of designing a HYPERbus-Novell gateway discussed above. DECnet is a close variant of a pure 802.3 CSMA/CD network; hence it shares all of the connectivity problems present in the HYPERbus-Novell design.

Table 2 summarizes the differences in architecture between the DECnet and HYPERbus. Obviously, the problem of connecting these networks entails the same considerations as discussed in Section B.1. above. The only minor variation involves a slight difference in the frame format used by the DECnet as compared to the Novell.

Table 2: Comparison of DECnet and HYPERbus Architectures

CHARACTERISTICS	DECnet	HYPERbus
Transmission Techinique:	Baseband	Baseband
Topology:	Bus	Hierarchical Bus
Access Method:	CSMA/CD	CSMA/CD (virtual token)
Maximum Data Rate:	10M bps	10M bps
Transmission Media:	50 ohm coax	75 ohm coax
IEEE 802 standards:	partial 802.3	None
Type of Connection:	Connectionless	Connection-oriented

DEC's Data Link Layer produces a frame format (shown in Figure 8) that contain a synchronizing header, a six byte destination address, the data from the user message, and a 32-bit cyclic redundancy check. Valid frames contain at least 64 bytes. [Ref. 5]

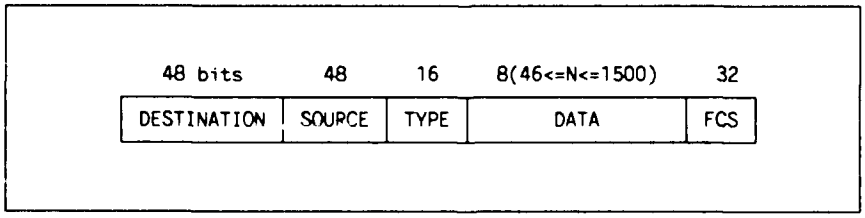


Figure 8: DECnet Frame Format [Ref. 14:p. 64]

DECnet addressing and routing functions are handled somewhat differently when multiple LAN's are tied together to form an internet than they are in an isolated network. In such cases, the address for a DECnet node is composed of a 16-bit number. The first six bits make up the area address for the node and the last 10 bits are used to identify the node number within that area. Area addresses can be any number from 0 to 63 and node numbers may range from 0 to 1,023. This combination of unique area-node number combinations allows DECnet to support up to 64,000 network/internetwork nodes. DECnet allows each node to define names for other nodes in the network and use these in establishing communications sessions in lieu of addresses. When a user on the network requests access to a node by its name, the session control software consults its address database and translates the name request to the correct numeric node address. This information is then passed to the end-to-end communications layer which establishes the logical link between nodes. [Ref. 5]

Despite the difference between the DECnet and Novell frame formats and addressing, the same general frame conversion and routing considerations described above for the Novell-HYPERbus gateway apply to the problem of achieving HYPERbus-DECnet connectivity.

In short, building a HYPERbus-DECnet gateway is a problem of the same technical complexity as discussed for a HYPERbus-Novell gateway design. It is highly questionable that constructing such a gateway is possible and the

customized solutions required are likely to be quite costly. Fortunately, other connectivity alternatives exist for building an NMPC internet.

C. DECNET CONNECTIVITY.

An alternative to building an NMPC internet around the existing HYPERbus infrastructure is to use the planned DECnet backbone (expanded as needed) to connect the Novell LAN's, existing DECnets, and the IBM mainframes. This could be implemented in parallel with the HYPERbus or the HYPERbus could be phased out with its devices being transferred to the DECnet backbone. The advantages and disadvantages of these overall alternatives are discussed in the following chapter while the specific connectivity devices required to accomplish them are outlined below.

DECnets are uniquely well suited to large LAN implementations and the internetworking of multiple ethernet LAN's (e.g. NMPC's Novell nets). DECnet's ability to work in multi-vendor environments and intermix PC based networks with mini and mainframe environments makes it an excellent candidate for use in meeting NMPC's internetworking requirements. A detailed treatment of the DECnet architecture is presented in Appendix G and may prove a useful reference in considering the discussion presented below.

1. DECnet - Novell Gateway (Bridge).

For all the complexity associated with HYPERbus connectivity, solutions centered around a DECnet backbone are essentially trivial. Numerous

commercial products exist and may be obtained off-the-shelf to achieve the desired connectivity. Nevertheless, some minor considerations merit discussion. Table 3 on the following page compares the DECnet and Novell architectures as they are currently implemented and as they will be in the near future.[11] Connectivity requirements between DECnet IV (the current DECnet implementation) and Novell 802.3 networks are fairly simple and easily achieved with proven gateway products. DECnet V, the upcoming DECnet implementation is fully OSI compliant and will reduce DECnet - Novell connectivity requirements to those of a simple bridge.

a. DECnet IV - Novell Gateway.

Although DECnet IV is very close to Novell's 802.3 architecture there are some differences which a gateway would need to resolve. Specifically, DECnet's ethernet implementation and that of the Novell net (ISO standard) differ primarily in the structure of individual data packets. The DECnet IV packet (Figure 8 above) must undergo a conversion to be recognized by the Novell network. This conversion is relatively straightforward and easily accomplished by a gateway. The conversion occurs in an OSI sublayer referred to as the subnet enhancement layer. This layer offers the services necessary to adjust the characteristics of a subnet's data frames to meet the requirements of transfer across the internet [Ref. 11:p. 322].

[11]Both Novell and DEC have announced the release of new versions of their current architectures to be released this year (1990). These versions are fully compliant with OSI/GOSIP standards and therefore will be easily interconnected. [Ref. 15, Ref. 16]

Additional gateway functions are also performed in Layer 3. DECnet uses slightly different routing algorithms than does Novell [Ref. 5]. Therefore, The gateway must be designed to resolve these differences through a conversion process. This process normally takes place in an OSI sublayer called the subnet access layer which reconciles the differences in network layer services between the subnets [Ref. 11:p. 322].

A further difference in DECnet IV's architecture and that of Novell lies in its End-to-End Communications Layer which corresponds to the OSI Transport Layer and performs similar functions; however, it does not use ISO protocols in doing so. Thus, the gateway must also provide services to reconcile these differences. [Ref. 5]

The differences pointed out between the DEC and Novell nets are relatively minor and some may even argue that the gateway connecting them might more appropriately be called a bridge. However, because there are in fact differences that must be resolved between the networks, it appears more appropriate to consider the connectivity device a gateway. For the interested reader, the differences between bridges and gateways are fully described in Appendix F.

b. DECnet V - Novell Bridge.

The impending release of Phase V will improve DECnet's capability as a truly open systems networking architecture. It is engineered to facilitate internetworking through compliance with OSI standards including exact

compliance with the ISO standards for Ethernet networks (ISO 8802-2, 8802-3). As a result, DECnet V - Novell connectivity will be easily accomplished through the use of a simple 802.3 bridge as described in Appendix F. [Ref. 15]

This full compatibility with Novell is the result of significant standardization of the DECnet V implementation. For example, its Network Layer will route user data between network systems through the use of the ISO Internet Protocol (ISO 8473) and its Network Layer will provide for various kinds of communications to support internetworking with broad spectrum of diverse vendors' networks. DECnet's V's upper layers make full use of some standardized applications protocols, such as the X.400 message system and the File Transfer, Access, and Management (FTAM) standards and its Application Layer allows the implementation of user defined applications for accessing and managing network resources. Applications available from DEC for this layer include network office systems, computer conferencing, remote database access, virtual terminal operations, SNA interconnection, network management, electronic mail, system services, and file transfer. [Ref. 15]

As is evident from the above discussion, DECnet V is designed to easily upgrade DECnet IV systems and meets OSI/GOSIP standards. This makes it a truly open system that is extremely well suited for use in meeting NMPC's internetworking requirements.

2. DECnet - IBM Gateway.

Key to the use of a DECnet backbone in lieu of the HYPERbus is its ability to support terminal emulation and full interconnectivity with NMPC's IBM mainframe resources. This is one of the DEC network architecture's greatest strengths with a broad range of DEC-SNA (IBM) gateway products available off-the-shelf. Digital produces gateways consisting of both hardware and software products that provide a virtually transparent exchange of data between DECnet and IBM SNA environments. Such gateways allow VAX-run applications programs to communicate in an IBM network using IBM protocols. Most significantly, DECnet IV allows DECnet terminals to emulate IBM terminals and access IBM applications. Under DECnet, a VAX can process jobs for IBM mainframes and thus act as IBM remote job entry systems. NMPC's Novell networks could also enjoy full access to the IBM environment once gatewayed (or bridged) to the DECnet. This is feasible under DECnet IV and will be even more easily accomplished with the release of DECnet V. Thus, under the DECnet architecture there is an established capability for achieving the IBM connectivity required of an NMPC internet making DECnet based alternatives easy to implement.

3. NMPC Connectivity with the NHPS Classified DECnet.

NMPC's unclassified NHBS DECnet system is a companion system to the classified NHPS DECnet located in the Pentagon two miles from the Navy Annex (NMPC). During the on-site interviews conducted in support of this

study, representatives of NMPC-163 expressed an interest in connecting the NHPS classified DECnet with either NMPC's classified HYPERbus or the unclassified NHBS DECnet (via the planned unclassified DECnet backbone). Since these questions concern NMPC's classified systems, they will not be fully addressed here. However, some general observations may be made.

The feasibility of a classified HYPERbus - classified DECnet gateway is as problematic as that of the unsecured version discussed above. Its design would be complicated only slightly by the need to accommodate data encryption/decryption for secure transmission. The custom design and implementation of such a gateway would face all of the technical challenges discussed above and since security considerations add an additional facet to the problem, it would likely be more costly than the unclassified gateway.

Connecting the classified DECnet to the unclassified DECnet backbone represents an entirely different problem. The actual connection of these networks could be easily accomplished through a standard DECnet bridge. However, it is the opinion of this study that doing so represents and unacceptable security risk. Bridging an unclassified system to a classified system would require extraordinary measures to guarantee effective access control. It may be possible to preclude access to certain nodes, prevent decryption of classified traffic on the unclassified net, and take other security precautions. Nevertheless, networking technology is not foolproof and providing interconnectivity between a classified and unclassified net presents an increased

risk of unauthorized access. Therefore, such interconnectivity should not be pursued.

D. DEVELOPING ALTERNATIVES FOR AN NMPC INTERNET.

The above discussion has provided a broad overview of the technical considerations of the potential system-to-system connections which might be used in building an NMPC internet. However, not all of these gateways and bridges need be used to achieve NMPC's internetworking goals. The next chapter discusses three alternative internet configurations suited to NMPC's requirements and built from the connectivity devices discussed above and makes recommendations for NMPC's transition and target internet architectures.

VIII. INTERNET ALTERNATIVES AND RECOMMENDATIONS

A. INTRODUCTION.

The previous chapters have addressed technical aspects of interconnecting a variety of existing and planned NMPC information systems resources, but have not suggested what combination of these systems should be used to form an overall internet. The purpose of this chapter is to discuss alternative internet solutions and recommend transition and target technical architectures for NMPC to pursue. First, each of three alternative architectures is discussed and evaluated with respect to planning guidance (CNP CIRMP, CNP TAP, etc), technical feasibility, growth potential, economic considerations, and management factors. Second, characteristics common to all alternatives are briefly discussed. Finally, the chapter closes with recommendations for meeting NMPC's internet needs.

B. ALTERNATIVE 1: NOVELL OAN'S - HYPERBUS - DECNETS

This alternative is as shown in Figure 9. It connects existing Novell departmental LAN's and existing DECnets (NHBS) through gateways to the unclassified HYPERbus. It appears to comply with the CNP CIRMP's and CNP TAP's overall goals for achieving internet connectivity and should provide the required functionality outlined in Chapter 5. Note that this alternative does

not incorporate the planned DECnet backbone discussed in Chapter 6 and thus allows for the possibility that vendor protests and budget constraints may prevent its procurement.

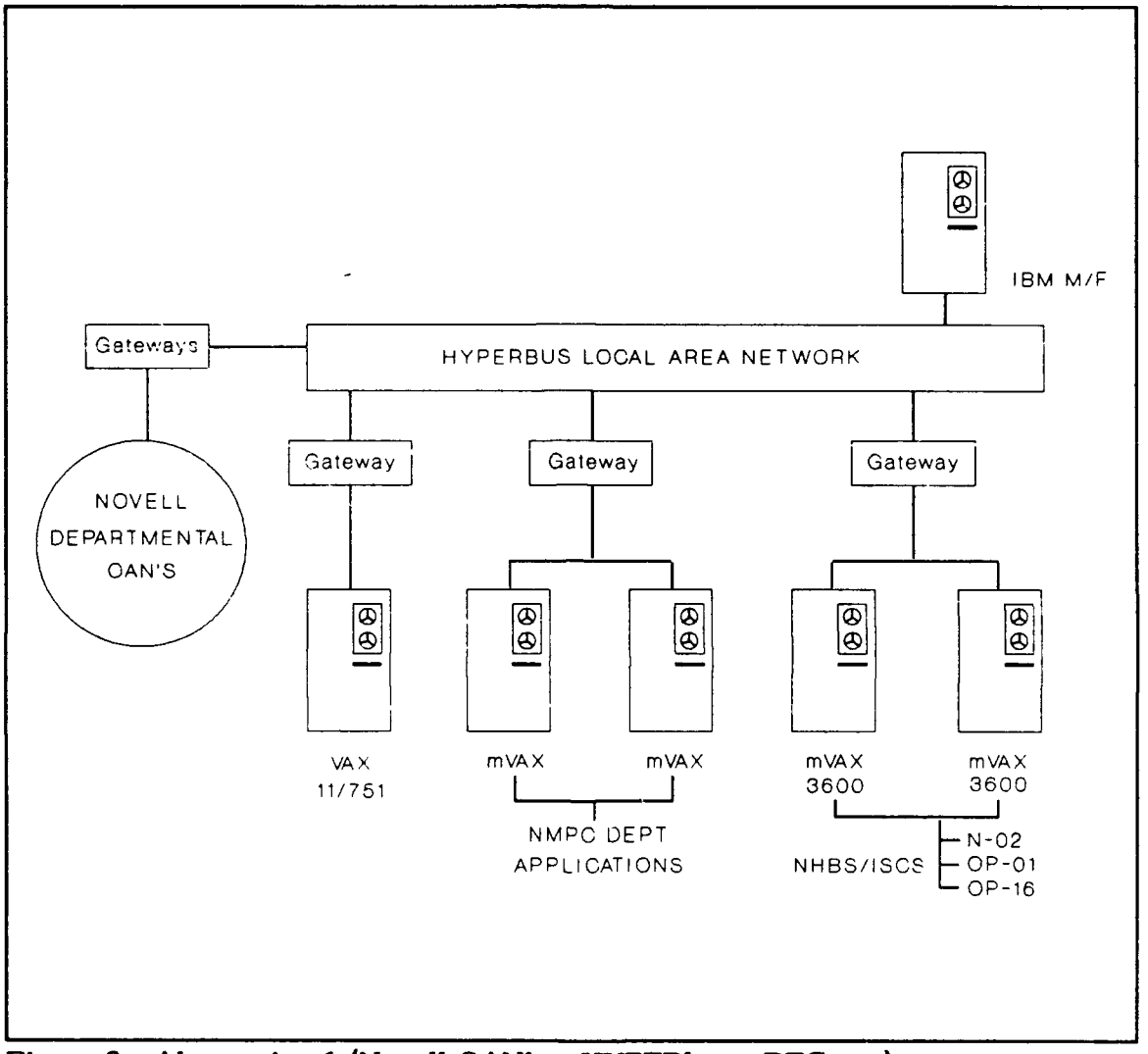


Figure 9: Alternative 1 (Novell OAN's - HYPERbus - DECnet's)

The CNP TAP defines six planning factors (discussed in Chapter 4) that appropriately influence architecture planning: user/data requirements, capacity requirements, baseline configuration, resources, technology, and standards. The

degree to which this alternative meets each of these factors is an effective means of evaluating its merit and potential to meet NMPC's needs.

1. User/Data Requirements.

As discussed in Chapter 5, the internet must meet several basic functional requirements: E-mail, file transfer among departmental nets, and mini/mainframe access for remote processing and file transfer. All elements of this alternative are capable of performing these functions provided the extraordinary technical solutions discussed in Chapter 7 are implemented.

2. Capacity Requirements.

It is difficult to estimate whether or not the HYPERbus has sufficient capacity to meet the additional demands of this alternative and still provide adequate response times. The HYPERbus currently supports approximately 1700 terminals, PC's, and printers [Ref. 4]. Under this alternative, approximately 1000 additional communicating nodes would be added to it and compete for its use.[12] These additional stations would significantly increase the volume of traffic sent across the network.[13] It is questionable whether the HYPERbus's CSMA/CA access control method is capable of handling this additional traffic

[12]This estimate of 1000 additional nodes represents the total number of workstations on existing Novell nets as summarized in Appendix 7 plus an estimate of DECnet workstations and OAN's planned for short term implementation.

[13]Although NMPC-167 believes that the HYPERbus could handle this additional capacity, our research suggests that it may not. Internets consisting of multiple networks often experience traffic management problems which cannot be accurately predicted without detailed study and simulations [Ref. 13].

without significant performance degradation. A detailed capacity study should be performed to determine the HYPERbus' capability to support additional traffic and reduce the performance risk involved in adopting this alternative.

3. Baseline Configuration.

The greatest strength of this alternative is the fact that it maximizes use of existing resources. There are some technical challenges of reliance on the HYPERbus as discussed in Chapter 7, but in the short term this alternative can meet NMPC's needs.

4. Personnel and Funding Resources.

Personnel availability and training requirements are negligible factors in evaluating this alternative. Since it is built around existing systems, little additional training will be required. Staff increases should not be required since network management and maintenance functions should be well within the capabilities of existing network managers and NMPC-167 personnel. Redefinition of responsibilities and reorganization to form an internet support group within NMPC-167 may be necessary, but should not require additional personnel.

Detailed cost analysis is beyond the scope of this study, however, some general observations can be made. In the short term, this alternative may be the least cost option. It makes use of the existing HYPERbus cable runs and therefore does not require costly cable installations. The gateways necessary to achieve Novell and DECnet connectivity to the HYPERbus will be more costly

than those of other alternatives. Since the HYPERbus is an uncommon system, the gateways needed will require custom development of the software and hardware configurations necessary to fully implement them. Similarly, the lack of off-the-shelf industry support for the HYPERbus will make modification of the system to meet future requirements more costly than other alternatives. Additionally, reliance on the relatively obsolescent components of the HYPERbus system will make maintenance more costly as well. Thus, although this alternative may require less funding up-front, its long term costs and limited potential for growth may make it less cost effective than other alternatives.

5. **Technology.**

As discussed above, this alternative relies heavily on obsolete HYPERbus technology giving it little potential to meet future requirements effectively. Since it does not adhere to open systems architectures such as OSI, GOSIP, etc., any future revisions of the system will probably require customized solutions at great contractual expense. In fact, the advantages of the DECnet and Novell network architectures which make them well suited to technological evolution, will be largely offset by their dependence on the HYPERbus. A system is only as strong as its weakest link and in terms of the ability to accommodate technological advances, the HYPERbus is a weak link indeed.

6. Standards and Guidance.

The fact that this alternative relies heavily on the HYPERbus runs directly counter to DOD requirements to migrate to standard network architectures. DOD directives require GOSIP compliance beginning in August 1990 [Ref. 17]. A waiver would have to be obtained in order to implement this alternative. The fiscal realities of a shrinking defense budget make it likely that a waiver request justified by reduced short term costs could be approved. However, adopting this alternative ignores the increased long term costs of non-compliance with emerging industry and government standards. Hardware and software developers are committed to OSI compliance and most research and development efforts are based on its recommended protocols and architectures. This means that widespread research and development efforts and vendor competitiveness will continue to reduce the cost of OSI compliant systems, while the contractor base to support non-standard systems will continue to diminish and thus increase in cost. Since this alternative does not comply with standardization initiatives, a decision to implement it would forfeit future flexibility and increase long term costs.

C. ALTERNATIVE 2: NOVELL-HYPERBUS-DECNET BACKBONE-DECNETS

This alternative is as shown in Figure 10. It connects existing Novell departmental LAN's through gateways to a DECnet backbone bridged to existing DECnets (NHBS). This backbone is then connected via a gateway to the

HYPERbus and NMPC's mainframes. This alternative appears to comply with the CNP CIRMP's and CNP TAP's overall goals for achieving internet connectivity and should provide the required functionality outlined in Chapter 7. Note that it assumes the successful procurement of the planned DECnet backbone discussed in Chapter 6.

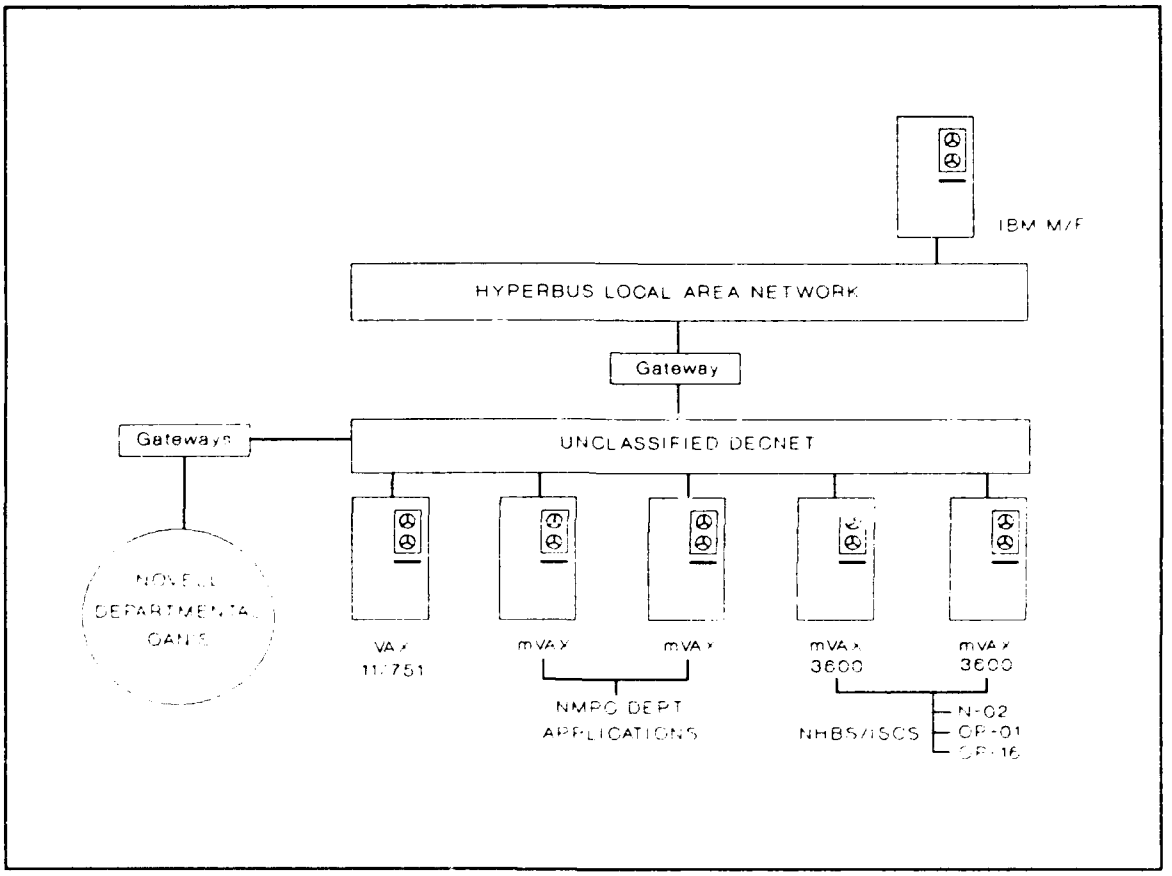


Figure 10: Alternative 2 (Novell's - HYPERbus - DECnet Backbone - DECnets)

The degree to which Alternative 2 meets each of the technical architecture planning factors outlined in the CNP TAP is discussed below and is an effective means of evaluating its merit and potential to meet NMPC's needs.

1. User/Data Requirements.

As discussed in Chapter 5, the internet must meet several basic functional requirements: E-mail, file transfer among departmental nets, and mini/mainframe access for remote processing and file transfer. All elements of this alternative are capable of performing these functions.

2. Capacity Requirements.

Similar to Alternative 1, it is difficult to estimate whether or not the HYPERbus has sufficient capacity to meet the expanded traffic demands of this alterative. It adds the same number of additional communicating nodes to the net as does the first alternative and requires the same studies to determine whether the HYPERbus is capable of handling this additional traffic without significant performance degradation. However, in Alternative 2, the Novell nets would make use of the DECnet backbone, and not the HYPERbus for inter-departmental communications. This is a significant difference from Alternative 1. Since the Novell nets have the least need for mainframe access, the majority of the traffic they generate would not traverse the HYPERbus. Thus, it appears that this alternative would not in fact increase HYPERbus traffic to the same degree as the first alternative. Since the DECnet backbone is unquestionably capable of handling the traffic it would experience, this alternative does not appear to run the risk of inadequate capacity inherent to Alternative 1.[14]

[14]DECnet V implementations are capable of handling tens of thousands of communicating nodes [Ref. 15]. This suggests that the proposed DECnet backbone can easily handle all present and foreseeable traffic demands.

3. Baseline Configuration.

This alternative makes good use of existing resources by preserving the HYPERbus and making it unnecessary to provide alternative support for its 1700 network devices. Although there are some technical challenges of continued reliance on the HYPERbus as discussed in Chapter 7, it is an effective existing system which presently meets its user's needs. Additionally, this alternative provides direct interconnectivity of the Novell and DECnet's, without the need to traverse the HYPERbus during communications between them. In this way, the strengths of these existing systems are not constrained by the weaknesses of the HYPERbus. Thus, this alternative preserves the strengths of all baseline systems without constraining the newer systems by full reliance on older ones.

4. Personnel and Funding Resources.

As in Alternative 1, personnel availability and training requirements have a negligible effect in evaluating this alternative. This alternative is built around existing systems with the addition of a DECnet backbone. Since this backbone merely represents another implementation of technology already in use by NMPC, little additional personnel training will be required. Staff increases should not be required since network management and maintenance functions should be well within the capabilities of existing network managers and NMPC-167 personnel. Redefinition of responsibilities and reorganization to form an internet support group within NMPC-167 may be necessary, but should not require additional personnel.

Some cost considerations are readily apparent. In the short term, this alternative will be more costly than Alternative 1. Although it makes use of the existing HYPERbus cable runs, it also requires the installation of a DECnet backbone which increases the cost of this option.[15] However, gateway costs should be reduced in this option, since only one HYPERbus gateway will be required for DECnet connectivity. Although this gateway will require custom development of the software and hardware configurations necessary to fully implement it, there will not be a need for the additional Novell-HYPERbus gateways involved in Alternative 1. DECnet-Novell connectivity will be easy to accomplish since both systems are to support OSI standards and commercial off-the-shelf gateway products should be available for use. As in Alternative 1, reliance on the relatively obsolescent components of the HYPERbus system are an additional cost factor of this option. Overall, the short term costs of this alternative will be greater than that of Alternative 1; however, long term costs may be reduced for the following reason. Since there is less reliance on the HYPERbus in this alternative, it may be possible to migrate away from it to the DECnet backbone as requirements change. Since under this option growth does not depend on overcoming HYPERbus obsolescence, it is likely that it may be more cost effective than alternative one in the long term.

[15]Such a backbone was planned for full implementation in FY 89 but has been indefinitely delayed by a vendor protest over the contract award.

5. Technology.

Although this alternative derives maximum benefit from the open systems' nature of its DECnet and Novell architectures, it still is handicapped by some reliance upon obsolete HYPERbus technology. The potential to overcome this handicap by migrating the HYPERbus' workstations/ devices to the DECnet backbone is a distinct advantage of this option over Alternative 1. The DECnet and Novell environments have far better potential for effective evolution to incorporate new technologies than does the HYPERbus.

6. Standards and Guidance.

The fact that this alternative still relies on the HYPERbus runs counter to DOD goals for standardizing network architectures; yet, its use of a DECnet backbone is a promising step toward GOSIP compliance. Nevertheless, it is only a half-step. Under this option NMPC will still experience the cost handicaps of using a non-standard system and will not be able to exploit the advantages of compliance with industry/government standards outlined in paragraph B.6. above.

D. ALTERNATIVE 3: NOVELL/DECNETS - DECNET BACKBONE - IBM'S

This alternative is as shown in Figure 11 on the following page. It connects existing Novell departmental LAN's through gateways to a DECnet backbone bridged to existing DECnets (NHBS). This backbone is then directly connected via a gateway to the NMPC's IBM mainframes.

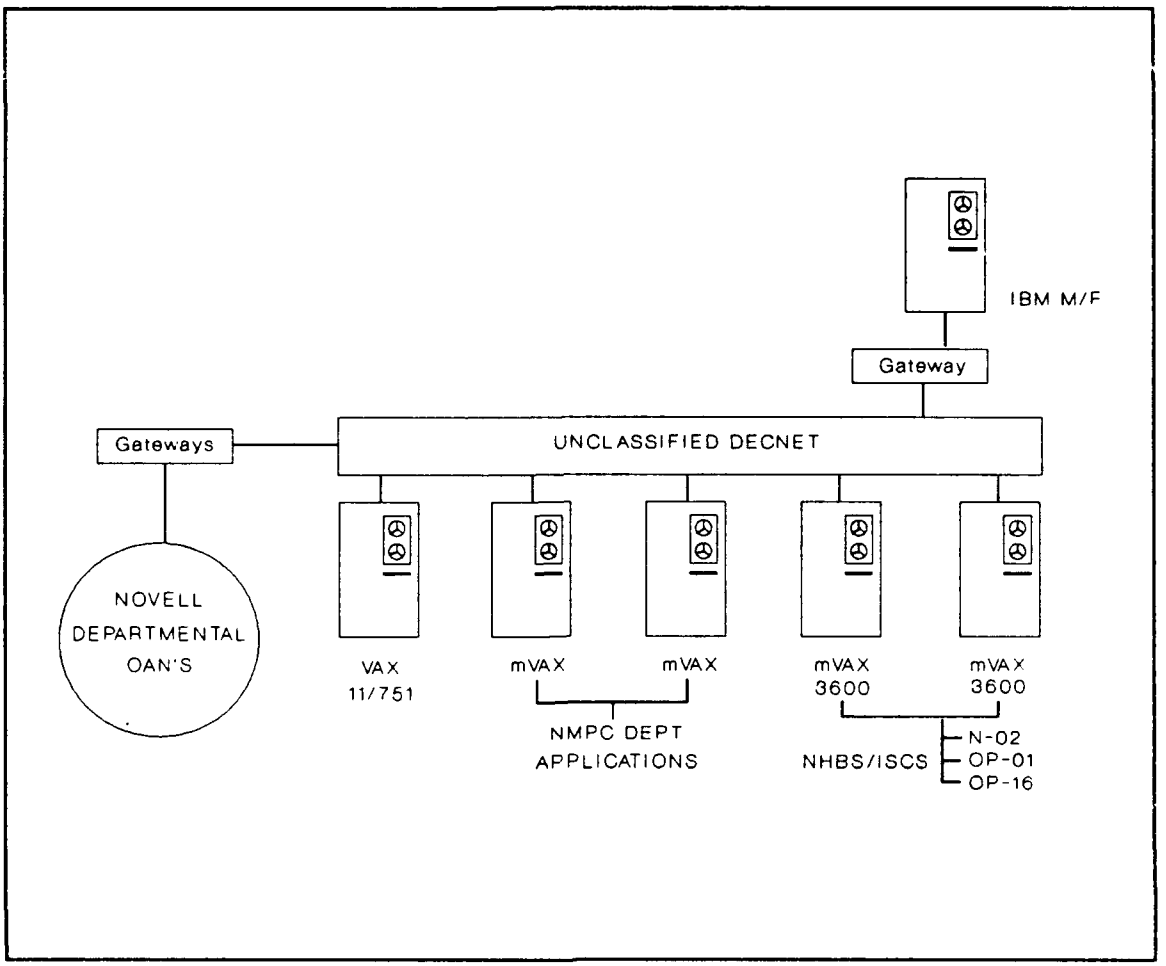


Figure 11: Alternative 3 (Novell/DECnets - DECnet Backbone - IBM's)

The key difference between this option and Alternative 2 is the elimination of the HYPERbus. Under this alternative a DECnet backbone is installed and connected through a gateway directly to the IBM mainframes. The HYPERbus is then gradually phased out with its devices being transferred to the DECnet backbone. This alternative appears to comply with the CNP CIRMP's and CNP TAP's overall goals for achieving internet connectivity and should provide the required functionality outlined in Chapter 5. It assumes the successful

procurement of a DECnet backbone sufficient to replace the HYPERbus and connect existing/planned Novell and DECnets.

The degree to which Alternative 3 meets each of the technical architecture planning factors outlined in the CNP TAP is discussed below and is an effective means of evaluating its merit and potential to meet NMPC's needs.

1. User/Data Requirements.

As discussed in Chapter 5, the internet must meet several basic functional requirements: E-mail, file transfer among departmental nets, and mini/mainframe access for remote processing and file transfer. All elements of this alternative are capable of performing these functions.

2. Capacity Requirements.

The proposed DECnet backbone is most probably capable of handling the combined traffic of the departmental LAN's, the connected DECnet's, and the devices formerly supported by the HYPERbus. Nevertheless, a study of traffic capacities could reduce uncertainty prior to phasing out the HYPERbus.

3. Baseline Configuration.

Selecting this alternative requires a conscious decision to eliminate the HYPERbus. In this respect, it is a significant departure from the baseline architecture and requires transferring the HYPERbus' approximately 1700 terminals, PC's, and printers to a new DECnet backbone. This eliminates the technical challenges of incorporating the HYPERbus into the internet but means securing authorization to phase out a working system.

4. Personnel and Funding Resources.

As in Alternative 1, personnel availability and training requirements have a negligible effect in evaluating this alternative. Although elimination of the HYPERbus has the potential of eliminating those personnel dedicated to its operation, the expanded internet will probably prevent a reduction in total personnel. Instead, those presently working with the HYPERbus may be expected to be shifted to duties involved with the operation and maintenance of the DECnet backbone. Since this backbone merely represents another implementation of technology already in use by NMPC, little additional personnel training will be required. Redefinition of responsibilities and reorganization to form an internet support group within NMPC-167 may be necessary, but should not require additional personnel.

Some cost considerations merit comment. In the short term, this alternative will be more costly than both Alternatives 1 and 2. It will require greater short term costs since it requires both the installation of a DECnet backbone and the transfer of HYPERbus devices to it. Gateway costs should be less in this option than in either Alternatives 1 or 2, since off-the-shelf commercial products are available for Novell-DECnet and DECnet-IBM connectivity. Its most significant long term cost advantages come in the complete elimination of the obsolete HYPERbus and hence a reduction in maintenance costs in comparison to the other two internet alternatives. It is easy to assert that long term costs will be reduced due to more flexible growth

potential and reduced operating/maintenance cost. Unfortunately, quantifying these savings will require subjective assumptions which may not be easy to defend. Therefore, it may be difficult, if not impossible, to justify the increased short term costs of this option in the environment of fiscal crisis now dominating DOD budgeting.

5. Technology.

This alternative represents the best opportunity to accommodate technological evolution. By eliminating the HYPERbus, the maximum advantages of open systems architecture may be realized. In terms of technological flexibility, this option far surpasses Alternatives 1 and 2.

6. Standards and Guidance.

Unlike either of the other options, Alternative 3 offers full compliance with GOSIP and entails all the benefits associated with a truly open systems environment. Since vendor development efforts may be expected to continue to build on the OSI standards this option supports, NMPC will be able to take maximum advantage of improvements in off-the-shelf products. This will mean lower long term costs in adapting the system to changing requirements and in reaping the benefits of software and hardware improvements.

E. CHARACTERISTICS COMMON TO ALTERNATIVES 1, 2, AND 3.

Each internet alternative will require NMPC-16 to establish organizational mechanisms to manage, maintain, and provide for security of the internet.

Security considerations will be particularly important, for although this study only addresses the internetworking of systems handling unclassified data, there are still requirements to restrict and control access. It appears that all of the alternatives discussed above allow for adequate security controls to be implemented. However, since HYPERbus is an older system, its security provisions are less flexible than those of the Novell and DECnets. Therefore, the relative ease of implementing security controls is directly related to the degree of dependence on the HYPERbus of each internet alternative. Accordingly, Alternative 3 offers the best security provisions with Alternative 2 being slightly better than Alternative 1.

One other aspect common to all three alternatives is the need for access to systems external to NMPC Headquarters. This is currently accomplished through a wide range of dial-up communications over commercial and dedicated lines. Although a detailed discussion of NMPC's wide area network (WAN) requirements is beyond the scope of this study, it should be pointed out that DOD directives require that such telecommunications requirements be migrated to the Defense Data Network (DDN).[16] Accordingly, the ease of accomplishing DDN connectivity is a common consideration for all three alternatives. DDN gateways exist for Novell, DECnet, and IBM systems and a variety of systems

[16]The migration to the use of DDN where appropriate is mandated by DOD directive. The DDN Mandate issued 10 March 1983 has been supplemented by DON implementing directives which require NMPC to develop a DDN capability as earliest as practicable. [Ref.4:p. 71]

are commercially available for them.[17] However, the prospects for HYPERbus-DDN connectivity are not as readily supported and would require custom development. This is yet another factor in favor of the internet options which reduce NMPC's reliance on the HYPERbus (principally Alternative 3).

F. INTERNET RECOMMENDATIONS.

If long term cost effectiveness is the decisive factor in selecting an internet alternative, then clearly Alternative 3 should be implemented. By phasing out the obsolescent HYPERbus and basing the internet on DECnet and Novell configurations, all of the benefits of open systems architectures complying with OSI standards are realized. The long term advantage in standards compliance is well recognized by the government as indicated in its formulation of the GOSIP standards and the directives requiring GOSIP compliance in all system implementations. However, the cost-cutting realities of the present fiscal environment combined with uncertainties about the size and organization of the Navy (and hence questions about NMPC's future mission requirements) probably make immediate adoption of Alternative 3 unlikely. Nevertheless, NMPC should resist yielding to short term pressures at the expense of long term cost effectiveness and work toward the implementation of Alternative 3. It

[17]GSA schedule contracts exist for a variety of equipment configurations supporting such gateways. For example the 1989 SMS Data Products Group, catalog of GSA schedule items specifies a microcomputer based DDN gateway for Novell LAN's. [Ref. 18:p. 34]

represents the most flexible solution and promises to most effectively meet NMPC's future needs.

Unfortunately, it is far more reasonable to expect the approval and implementation of Alternative 2, since it has lower short term costs and allows partial compliance with GOSIP standards. An additional advantage of adopting Alternative 2, is that it allows HYPERbus to be phased out at some point in the future (in effect becoming a delayed implementation of Alternative 3). These factors make it likely that Alternative 2 will be selected despite the fact that continued commitment to HYPERbus will complicate maintenance and operation of the internet and probably result in a long term cost which is actually greater than that of Alternative 3.

Whichever alternative is selected, the effectiveness of its implementation will depend on NMPC's approach to network planning and information systems management. During the course of this study, many strengths and some weaknesses were identified in NMPC's network planning structure. The remainder of this paper addresses management issues. First, Chapters 9 and 10 examine the NMPC status quo and make recommendations for its improvement. Second, Chapters 11 and 12 identify generally applicable lessons learned in studying NMPC and apply them in making recommendations for network planning and development useful to other DOD organizations facing internet design decisions.

IX. NETWORK PLANNING AND DEVELOPMENT IN NMPC

A. INTRODUCTION.

Identifying feasible technical architecture alternatives does not in itself guarantee successful development and implementation of an effective NMPC internet. It is important to recognize that the way NMPC manages its information systems planning and development will be a key factor in successfully building a comprehensive internet.

Both the CNP CIRMP and CNP TAP portray a target information systems environment for NMPC in which a multitude of local area networks are interconnected to form an effective, organization-wide internet allowing access to mainframe resources and achieving effective resource sharing in support of corporate systems while fostering departmental end-user computing initiatives. The challenges of constructing such system will require careful planning and development. The continuing procurement and installation of office area networks must be managed with an eye toward facilitating internetwork connectivity while making the best possible use of limited funding and organizational resources. This chapter critically examines NMPC's current organizational approach to network planning and development.

B. ORGANIZATIONAL RESPONSIBILITY.

The need for clearly defined organizational responsibilities and centralized management of departmental initiatives is indisputable. Yet, our study suggests that NMPC's detailed systems implementation planning has not yet reached maturity. Although NMPC's managers are performing miraculously well under current organizational constraints, systemic problems prevent adequate long range planning to meet internetwork connectivity requirements. Most significantly, a planning void exists in which departmental local area networks proliferate without adequate provision for interconnectivity among them nor for interfaces with wide area networks and mainframe resources necessary to meet the overall goals of the CNP Claimancy.

NMPC-16, the Total Force Information Systems Management Department, has overall responsibility for all facets of NMPC's internal information systems planning and management. Under its current approach to the planning and implementation of networks, two of its subordinate elements play leading roles: NMPC-163, the Customer Support Division and NMPC-167, the Technology Support Division. However, its other sections do not appear as involved despite a need for their input.

A review of the CNP CIRMP and CNP TAP suggests that network planning should be performed to ensure that implemented systems will meet the requirements of distributed processing in support of corporate databases and field systems now undergoing development. Initiatives to define NMPC data

elements, design corporate databases, and build effective field systems are on-going; being managed by NMPC-164, NMPC-165, and NMPC-166 respectively. This suggests that these departments should play at least an advisory role with respect to network planning and development. However, our study found little evidence of formal or informal organizational mechanisms to provide for their involvement. Rather, network planning and implementation functions appear to be occurring in both NMPC-163 and NMPC-167 but without adequate coordination between the two and little input from other departments.

C. NETWORK PLANNING.

In conducting the on-site survey and interviews which form the basis for this study, it was not possible to identify a single office within NMPC-16 which had overall responsibility for the integration of the diverse corporate and departmental systems being developed by its subordinate sections. As a result, it appears that although the CNP CIRMP and CNP TAP together provide a clear overall information systems goal in broad terms there is no organizational element within NMPC which is coordinating the technical details of its major systems initiatives.

From the independent perspective of this study, it appears that the Director and Deputy Director effectively manage the overall direction of the various programs for which NMPC-16 has responsibility. Similarly, their subordinate sections appear to be aggressively, and effectively managing the detailed

development of the systems for which they have responsibility. However, there does not seem to be any effective organizational mechanisms for ensuring their efforts move in compatible directions. For example, planning by NMPC-167 forecasts the demise of the HYPERbus emphasizing its inability to meet standards necessary for cost-effective interconnectivity with dissimilar nets and its relative obsolescence from an industry standpoint.[18] Simultaneously, NMPC-163, tasked with supporting departmental network initiatives, is planning internetwork connectivity using the HYPERbus as their centerpiece solution [Ref. 20, Ref. 21].

Further examination of this issue explains how such a discrepancy may exist under NMPC's current approach to network management and planning. The day-to-day operation of the HYPERbus is managed by NMPC-167 who provides technical supervision and support of the network but does so in a service role only. It connects DTE's, coordinates maintenance, and plans for the acquisition of network devices as necessary. It is not directly involved in planning the connection of additional systems to the net. Rather, it is merely advised of changes in net utilization and assists in implementation when tasked to do so. Meanwhile, NMPC-163 plans the addition of devices to the HYPERbus in accordance with its vision for a comprehensive internet. In doing so, it appears

[18]NMPC-167's perspective on the HYPERbus is documented in a NMPC-1672 memorandum, dated 27 June 1989, Subject: Telecommunications Policy [Ref. 19] Interviews with Bean and Scarano during the site survey conducted in September 1989, confirmed this position and revealed that NMPC-167 was largely unaware of NMPC-163's plans for using the HYPERbus as a part of an overall internet connectivity solution. [Ref. 7, Ref. 19]

not to have a clear program for evaluating the HYPERbus's technical capability to accommodate its plans. Capacity studies, compatibility issues, and the plan's effects on network reliability and responsiveness have not been adequately explored. Although NMPC-167 might logically perform these tasks, it remains largely unapprised of NMPC-163's plans and consequently provides little input.

The HYPERbus is just one example of the need to coordinate network planning functions more effectively. NMPC must develop a means by which the planning activities of its departments are managed to complement, and not counteract each other. The independence exercised by NMPC-16's subordinate departments may not often produce problems evident in the short term accomplishment of individual objectives; but, ultimately, this independence will impede the integration of diverse elements into a comprehensive, corporate information system. There is clearly need for change. Recommendations for improving NMPC's organizational planning structure are outlined later in this study.

X. IS MANAGEMENT RECOMMENDATIONS

A. INTRODUCTION.

Chapter 9 outlined some of the strengths and weaknesses of NMPC's current approach to the procurement and installation of office area networks. For NMPC to develop and implement a comprehensive internetwork of these systems, it is essential that management activities be better coordinated. The purpose of this chapter is to outline specific measures NMPC may take to improve its network planning process and facilitate the development of effective information systems to meet the goals of the CNP CIRMP and CNP TAP.

B. THE STATUS QUO.

As discussed in Chapter 9, NMPC-16, the Total Force Information Systems Management Department is responsible for information resource management within NMPC. Under its current approach to the planning and implementation of networks, two of its subordinate elements play leading roles: NMPC-163, the Customer Support Division and NMPC-167, the Technology Support Division. Each performs functions affecting network planning but without adequate coordination between them and little input from other departments despite a need for their involvement. Specifically, initiatives to define NMPC data elements, design corporate databases, and build effective field systems are being

managed by NMPC-164, NMPC-165, and NMPC-166 respectively. These programs will clearly affect network functional requirements, yet, our study produced no evidence of any formal or informal organizational mechanisms to provide for their input in the planning and implementation of departmental networks.

NMPC must develop a means by which the planning activities of its departments are managed to complement, and not counteract each other. The independence exercised by NMPC-16's subordinate departments may not often produce problems evident in the short term; but, ultimately, this independence will impede the integration of diverse elements into a comprehensive, corporate information system. Clearly, there is a need for change if the internetwork recommendations presented in Chapter 8 are to be implemented effectively.

C. STRENGTHS AND WEAKNESSES OF THE STATUS QUO.

NMPC's individual managers are doing an excellent job of identifying current requirements and providing for their solution. NMPC-163 has been exceptionally effective in orchestrating the planning and procurement of a multitude of departmental office area nets. However, for all the strengths of individual managers there are several organizational weaknesses which weaken long term planning effectiveness and therefore require correction.

First, consider the strengths our study found in current network planning efforts. NMPC-163 has developed clear standards for office automation

hardware and software which facilitate LAN implementation and will aid in the effective interdepartmental exchange of data across the internet once implemented.[19] In designing and approving office area networks, NMPC-163 has meticulously required adherence to established standards. Most notably, it has ensured that all OAN's are built around a common standard (802.3 specifications) and use common network management software (NetWare). Because of their foresight in dictating and enforcing this requirement, the technical task of integrating these networks is easily achievable, despite the fact that constraints of the procurement system have led to a conglomeration of diverse vendor products throughout NMPC. NMPC-163's foresight in selecting the 802.3 standard not only facilitates the interconnection of the Novell OAN's, it also facilitates the incorporation of the NHBS and other DECnet systems. This adherence to established standards contributes more to NMPC's ability to construct an effective internet than perhaps any other single factor identified in this study.

Another significant strength of NMPC-163's approach to fostering end-user computing, is their responsiveness to user requirements and their willingness to build office area networks tailored to each departments unique requirements. However, although this is a strength in that it improves user involvement and increases the effectiveness of implemented systems, it also has led to some

[19]These standards provide for a wide range of effective office automation tools including WordPerfect, DBase IV, Harvard Graphics, Lotus 1-2-3, and Enable. [Ref. 22]

dangerous precedents and potential pitfalls. For example, the ASDP for NMPC-132's OAN indicates that the use of Macintosh computers as the primary network workstations was allowed. Although there is nothing wrong with the use of Macintoshes from the perspective of a single department, it is questionable whether such diversity is effective in the face of requirements for MS-DOS compatibility to interact with the vast majority of NMPC's departmental systems. The ASDP for this network went to great lengths to assert MS-DOS compatibility (despite technical factors which suggest otherwise) and the final implementation incorporated a specially configured Zenith-248 as a communications server to allow the exchange of information with other systems. The extraordinary effort required to incorporate Macintoshes was justified by the department's claims of ease of use and the need for integrated text and graphics. However, NMPC-132's requirements are not significantly different from those of NMPC's other departments making this argument far from compelling. It appears that the purchase of the Macintoshes was more a result of an eight week loan of several systems by an interested vendor, than by a clear need for their unique capabilities.[20]

In allowing the purchase of Macintoshes, NMPC-163 acted in accordance with the goals of the CNP CIRMP which encourages end users to take the lead in developing their information systems and allows the acquisition of non-

[20]These conclusions represent the authors' interpretation of information presented in the ASDP and accompanying documentation for NMPC-132's OAN [Ref. 23].

standard equipment. However, this case represents a deviation from standards that will complicate interconnectivity requirements needlessly. It is a dangerous precedent and represents a weakness of the present approach. NMPC-163 should have clearer authority to prevent deviation from established standards unless exceptionally unusual and unique requirements make such variations absolutely necessary.

This points out a similar systemic weakness. NMPC-163 is the Customer Support Division and is tasked with supporting end-user requests. There is nothing wrong with its role as a support division; however, there appears to be a tendency for this role to cause short term customer needs to dominate network planning and development without adequate consideration of long term system requirements. Specifically, in reviewing the ASDP's of implemented office area networks, the storage and processing requirements of servers and workstations were universally determined by departmentally specific requirements alone. There is no evidence that resource requirements associated with the systems initiatives being pursued by NMPC-164, 165, and 166 were considered in determining OAN resource requirements. These sections are working on data definition for corporate systems and distributed processing, as well as the design of field systems with which NMPC departments will be required to share information. These initiatives have the potential of requiring storage and processing resources in departmental networks beyond those acquired based on user requests. As a result, OAN network resources may prove inadequate to

meet the needs of the comprehensive, NMPC information system envisioned by the CNP CIRMP and CNP TAP.

Another example of inadequate coordination between NMPC-16's sections is the failure of NMPC-163 and NMPC-167 to adequately work together in planning technical architectures. As discussed in Chapter 7, reliance on the HYPERbus as part of a comprehensive internet is problematic at best. The HYPERbus' technical limitations are well known to NMPC-167 and compelling reasons exist to decrease, rather than increase reliance upon it. Nevertheless, NMPC-163 does not appear to appreciate the HYPERbus' limitations and is planning to expand its use.

These examples of inadequate coordination between NMPC-16's sections should not be interpreted as a weakness of individual section personnel. On the contrary, individual managers demonstrate exceptional competence and dedication to working together. However, there is a systemic organizational weakness which leads to inadequate coordination. In conducting the on-site survey and interviews which form the basis for this study, it was not possible to identify one office within NMPC-16 which had overall responsibility for coordinating the diverse activities of its subordinate sections. As a result, it appears that although the CNP CIRMP and CNP TAP together provide a clear overall information systems goal in broad terms there is no organizational element within NMPC-16 which is coordinating the technical details of its major systems initiatives. In other words, each section works substantially in isolation,

when long term goals suggest that their efforts should be more closely coordinated. Clearly, there is a need to address this problem.

D. RECOMMENDATIONS.

NMPC-16 currently performs its information resource management functions exceptionally well given the Herculean scope of its responsibilities. Its dedication to standards, responsiveness to end-user requirements, and effective acquisition of systems despite a hostile procurement process are its most significant strengths. However, the lack of a specific organizational element tasked with coordinating the diverse, yet related activities of its subordinate sections produces inadequate planning coordination. Thus, the tyranny of the urgent and short term requirements have lead to the implementation of systems which may not be adequate to meet future needs. Correcting this deficiency is essential in order to transition NMPC's independent departmental systems into an effective comprehensive internet.

There are two potential solutions to this problem: creation of a formal organizational element to coordinate the activities of NMPC-16's subordinate sections or the formation of a matrix organization in the form of an ad hoc planning group. If a formal organizational element is created, it would need to exercise line authority over NMPC-163 through 167. The advantage of such an element is that responsibility for coordinating the activities of its subordinate sections is clearly fixed and there is no question over its authority to resolve

conflicts. On the other hand, it would represent an additional level of bureaucracy within NMPC-16 the effect of which might be counterproductive. Therefore, the use of the second alternative, the matrix organization is recommended. An ad hoc committee should be formed of the heads of NMPC-163 through 167 chaired by a senior representative of NMPC-16F, the Information Planning and Management Office. Since NMPC-16F is responsible for the CNP IRM process, it seems logical that this section should provide a chairman responsible for coordinating the ongoing activities of NMPC-163 through 167 to ensure their efforts are compatible and effective in moving the organization toward its long term goals. Specifically, the committee should be charged with providing for recommending, acquiring, and implementing the gateways necessary to build a comprehensive NMPC internet.

In administering the committee, the chairman should be charged with ensuring effective coordination between sections and have adequate authority to compel sections to respond to his directives. As a minimum, the chairman should have the authority to review activities of each section and compel periodic reporting of coordinating measures. The committee as a whole should meet no less frequently than once monthly with additional meetings called at the chairman's direction. It is important to emphasize that this recommendation requires the committee to be an operating task force which actively coordinates the initiatives of its members. If allowed to degenerate into just a figurehead organization, it will be ineffective, therefore, the

chairman should be required to report to the Deputy Director of NMPC-16. This will ensure that the Chairman receives adequate support from committee members in resolving conflicts and coordinating section activities.

XI. LESSONS LEARNED IN STUDYING NMPC

A. INTRODUCTION.

In studying NMPC, one finds several important lessons in information resource management (IRM) with applicability to other DOD organizations as well. Some are obvious and have been discussed in previous chapters, others are less obvious and merit further discussion. This chapter examines lessons learned in studying NMPC and covers issues ranging from strategic IRM planning to common pitfalls encountered in implementing information systems.

B. EFFECTIVENESS OF STRATEGIC PLANS.

NMPC has an excellent strategic IRM planning document in the form of the CNP CIRMP (discussed in Chapter 3). Admittedly, the scope of this plan goes well beyond NMPC, but it effectively describes NMPC's long term information systems goals. The heart of the document is the CNP IRM Program Six Year Scenario which prioritizes CNP IRM activities, serves as a planning tool for the budgeting process, and provides a framework for pursuing significant information systems initiatives. It defines a three phase program for implementing changes and appears to provide sufficient direction to ensure success. However, our study of NMPC reveals a disconnect between the CNP CIRMP and the day-to-day activities of NMPC's information resource management activities.

The CNP CIRMP has all of the elements of a good strategic plan. It establishes clear long range goals, analyzes current resources and on-going projects, recognizes environmental factors and constraints, considers the budgeting process, and presents a plan for achieving its objectives. Unfortunately, the further one gets from the committees and offices that assembled the plan, the less its objectives affect daily decision making. The CNP CIRMP is a good plan but its successful execution is being frustrated by the short range focus which dominates NMPC-16's subordinate sections. As discussed in previous chapters, this is the result of inadequate systemic controls to ensure that current efforts are adequately coordinated to remain consistent with the CNP CIRMP's strategic goals.

The lesson this teaches is that although effective strategic plans are necessary to achieve successful IRM management, they alone are not sufficient to do so. It is important to establish organizational and systemic structures to ensure that strategic plans are translated into action. The point may appear obvious, however, organizations too often assume that having a good plan guarantees effective execution.

Since many military organizations experience personnel turnover on a three to four year basis, there is a tendency for short term priorities to dominate decision making. It is hard for most individuals to maintain a long term focus when their success will be measured by short term results. Because of this tendency, it is extremely important to put systemic controls in place to ensure

that long term objectives are adequately considered in day-to-day operations and decision making. Such controls may take the form of formal organizational elements or ad hoc, matrix organizations as discussed for NMPC-16 in the previous chapter. But in general, the exact form of the controls is less important than the guarantee that some system be established to ensure that strategic plans are translated into coordinated action.

C. PITFALLS IN IMPLEMENTATION OF INFORMATION SYSTEMS.

Even when a good IRM plan exists, there are many pitfalls which managers may fall victim to in attempting its implementation. Evidence of several of these may be found in the study of NMPC. First, is the problem of coordinating diverse, yet related activities of the intermediate managers in a large organization. As previously discussed, NMPC-16's subordinate sections perform their individual duties exceptionally well; however, there are no adequate coordinating mechanisms to ensure their efforts complement one another. The lesson here is that as an organization's information systems needs become larger and more complex, formalized coordination procedures become more critical to effective management.

A second pitfall, disproportionate vendor influence, is also evident. The decision to acquire Macintosh computers as the workstations for NMPC-132's OAN appears to have been as much a function of the trial use of loaned machines as of a clearly defined need for their unique capabilities. Although

this single instance makes it a negligible problem for NMPC, it should form a valuable lesson for other DOD information systems (IS) managers. End-user computing initiatives are bound to become more and more common as computer literacy increases in an organization. IS managers must remain sensitive to the fact that most users will have a limited perspective on information technology driven by their individual exposure to computer systems. This means that users will often define their requirements in terms that support the acquisition of familiar systems and not necessarily optimal ones. IS customer support sections must understand that their role is to meet customer needs, not necessarily to respond solely to what users think they need. When assisting with the development of information systems, customer support personnel must recognize that users do not always know what's best. Additionally, responding to user needs must always be done with a broad organizational view to ensure that individual systems are planned to fit into overall information systems strategies.

A third pitfall that should be avoided is the tendency to remain committed to obsolete systems when it is no longer cost effective to do so. In NMPC's case, it may be argued that the long term costs of continued reliance on the HYPERbus will far outweigh short term savings. Even if this proves to be incorrect in the specific case of the HYPERbus, there is a valuable point to be made. As technology evolves it is important to fully consider both long and short term costs in making decisions to keep or abandon existing systems. Although this seems obvious, managers often fail to adopt a proper sunk cost

perspective in evaluating the continued usefulness of existing systems. This is particularly important to keep in mind in this period of shrinking DOD budgets. Decision makers have to seek the most cost effective solutions not the most cost expedient ones. In other words, care must be taken not to select systems which are cheaper in the short term simply because they have the best chance of surviving the budget process. Lifetime cost effectiveness must be the decisive factor. The challenge this presents is for resource managers to do a better job of quantifying costs and benefits to defend their proposals. Opting for the easy out of lower short term costs while ignoring lifetime cost effectiveness is a clear abdication of a manager's responsibility and a temptation which must be avoided.

D. THE VALUE OF ADHERING TO STANDARDS.

Perhaps, the single most effective aspect of NMPC's approach to the implementation of its information systems is its use of accepted government and industry standards as criteria for acquiring systems. Specifically, by requiring that all departmental OAN's meet 802.3 standards, NMPC-163 has significantly simplified the technical challenges of building a comprehensive internet. Similarly, NMPC-163 has reduced the cost of planning and implementing office area networks by identifying standard hardware and software for such implementations (the case of NMPC-132 excepted). NMPC-163's foresight has put NMPC in an excellent position for flexible future growth. Since hardware

and software developers are committed to OSI compliance, widespread vendor competitiveness will continue to reduce the cost of upgrading OSI-compliant systems making it easier for NMPC to modify its systems to meet future needs. This is an important lesson for other DOD organizations -- that adherence to standards will reduce long term costs.

E. APPLYING NMPC LESSONS.

The major lessons learned in studying NMPC are summarized as follows:

- Strategic plans must be accompanied by systemic controls to ensure they are translated into action.
- The larger the organization and the more complex its information systems, the greater the need for formal coordination mechanisms to ensure that short term decision making supports long range goals.
- Vendor influence may cause familiar systems to be acquired in lieu of optimal ones. Customer support sections must help users select what's best for them and the collective interests of the overall organization, not necessarily what individual users want.
- Lifetime costs of alternative systems must govern decision making. Sunk cost analysis should be used to avoid keeping to obsolete systems past the point of cost effectiveness. Budget constraints make it tempting to let short term costs guide decision making at the expense of long term cost effectiveness -- a pitfall to avoid.
- Identifying hardware and software standards and complying with OSI/GOSIP guidelines allows for flexible growth at reduced cost.

In examining these lessons learned, it is apparent that none of them are exceptionally insightful. Indeed, they merely confirm common guidelines most information systems managers have been taught in the past. Nevertheless, they

are often ignored in practice. It is far easier to recognize lessons than it is to apply them. In NMPC, one sees many strengths and weaknesses in its approach to information systems planning. Their organizational objective of creating a comprehensive internet is undoubtedly common to many DOD organizations. Accordingly, the final chapter of this study recommends a specific approach to internet planning and development that will help other DOD managers apply the lessons learned by NMPC.

XII. RECOMMENDATIONS FOR INTERNET PLANNING AND DEVELOPMENT

A. INTRODUCTION.

Rapid advances in information technology over the past several years have resulted in fragmented procurement and installation of systems throughout government organizations often without adequate long range planning. As a result, many DOD organizations find themselves with numerous independent systems and local area networks and a need to exchange information between them. Connecting local area networks into a comprehensive internet is one means of improving information sharing in an organization. This chapter defines the tasks associated with planning and implementing an effective organizational internet.

Setting up an internet of independent LAN's can be looked at as a series of hardware and software selection decisions. In its most basic sense the decision may be thought of as having two parts: identifying what needs to be done on the internet (its required functionality) and identifying what hardware, software, and interconnectivity structure will be necessary to build the internet.

B. IDENTIFYING REQUIRED FUNCTIONALITY.

The first step in building an effective organizational internet is to validate the need for such a system. It is a mistake to automatically assume that all of

an organization's information systems must be interconnected. Rather, it is important to clearly define the organizational requirements for information exchange before attempting to design an internet. This requires that a survey of information flow within the organization be performed. This study should work to determine what information is exchanged between which organizational elements and in what form, volume and frequency. In determining this, it is important to identify where data resides in existing information systems and evaluate whether the on-line exchange of data is the most effective means of doing so. Once the organization's information flow has been determined, it is important to identify the processing functions the internet must perform such as file transfer, terminal emulation, E-mail, etc.

Gathering this information is best accomplished by consulting the users of existing systems and the potential users of the projected internet. Thus, formation of a user's committee of representatives of each organizational element is an effective catalyst for determining required information flow. In forming such a committee, it is important that its representatives be thoroughly familiar with the types and nature of data used on a daily basis.

A second purpose of the Users Committee is to help overcome resistance to change. This is an important managerial consideration. Existing systems have users who will resist changes which they perceive may adversely effect the way they do business; therefore, the information system manager who seeks to develop an effective internet must involve users in the process of its

implementation. Designing an internet around existing resources requires balancing individual user needs with overall organizational goals. By involving effected elements through their role in the User's Committee, the information systems manager will foster greater support for the transition to an organization-wide internet.

C. IDENTIFYING HARDWARE/SOFTWARE & CONNECTIVITY REQUIREMENTS

Once the internet's functional requirements have been determined, attention turns toward hardware, software, and connectivity issues. Here the first step is to identify the components of existing systems. This may be a more difficult task than it originally appears, since in large organizations many of the existing systems will have been acquired in separate procurements. The government procurement process is such that it is likely that existing systems will include a wide variety of diverse hardware and software from many different vendors. Therefore, as information is gathered on the local area networks to be connected, special attention should be paid to determining to what degree existing systems comply with open systems standards. The greater the compliance with established standards (OSI/GOSIP), the easier construction of the internet will be. Specifically, the hardware and software in use on each LAN should be determined and the network architecture should be outlined in terms of transmission media, topology, and methods of access control.

Once the architectures of existing LAN's have been clearly identified, they

should be compared to determine the extent to which they differ. This will provide the starting point for identifying interconnectivity requirements and determining the technical feasibility of various solutions. LAN's which comply to OSI/GOSIP standards may often be connected using off-the-shelf products to build the routers, bridges, or gateways necessary to tie them together in an internet. On the other hand, non-standard LAN's will often require customized gateways to interconnect them. This adds an additional variable to be considered. In some cases, it may be more cost effective to abandon non-standard or obsolete systems than to develop the complex gateways necessary to incorporate them in the internet. Security factors, distances to be covered by the internet, and other physical constraints (space limitation, building ventilation, wiring, etc.) should also be considered when developing alternative internet configurati ns.

The next step is to perform a cost-benefit analysis of each internet alternative. The ultimate selection of a particular alternative should be made on the basis of long term cost effectiveness over the anticipated lifetime of the system and not on the basis of short term costs alone. DOD budgets will be severely limited in the years to come making it imperative that IS managers select the most economic internet solutions. Following GOSIP guidelines is an important means of ensuring that systems will remain flexible to accommodate evolving requirements and allow economical growth over time.

D. IMPLEMENTING THE INTERNET.

Once a cost effective, technically feasible internet design has been determined, implementation may begin. The information systems manager must ensure that this process not only includes the procurement and installation of necessary systems, but also includes personnel training, and provisions for the operation, maintenance and management of the internet. When an organization transitions from multiple LAN's working independently, to a single, comprehensive internet, network management becomes far more complex. Security issues, data access, maintenance, and the addition and removal of workstations all require careful management if the internet is to remain effective. Depending on its size, the implementation of an internet may require significant dedicated personnel resources to keep it operating effectively. Therefore, consideration should be given to forming an organizational element to administer the internet prior to its activation. On the other hand, some organizations may find it possible for existing IS support elements to perform internet management. In either case, the information systems manager must determine what network management measures will be required and provide adequate resources to do so.

E. SUMMARY OF THE STEPS RECOMMENDED IN BUILDING AN INTERNET.

The steps involved in building an effective internet of existing LAN's are summarized as follows:

- Validate the need for an internet and identify the goals it is to accomplish by analyzing the organizational structure and flow of information throughout the organization.

- Form a users committee of knowledgeable representatives to assist in determining the required functionality of the internet. Identify what information is to be exchanged between which organizational elements and in what form, volume, and frequency. Identify the applications required such as file transfer, terminal emulation, etc.

- Identify existing resources. Determine the architectures of existing LAN's in terms of transmission media, topology, and access control methods.

- Identify the degree to which existing LAN's meet open systems standards and determine the technical feasibility of routers, bridges gateways or other devices necessary to interconnect them and accomplish required internet functionality.

- Identify constraints such as security factors, distances to be covered, space limitations, etc. Develop feasible alternative internet configurations.

- Perform cost-benefit analysis of each alternative and select the most cost-effective configuration. Ensure cost analysis is performed from an appropriate sunk cost perspective and that decisions are made on the basis of lifetime costs and not solely on short term considerations.

- Oversee implementation of the selected internet solution. Ensure that adequate training occurs and establish organizational responsibility for the operational management and maintenance of the internet.

The internet needs of each organization are different and there are no simple solutions for connecting diverse LAN's. Building an effective organizational internet requires detailed planning and careful management. The steps outlined above will help an IS manager to arrive at an effective internet solution. The most important aspect to keep in mind is that technology will

continue to evolve and those internet's built to comply with accepted open systems architectures (OSI/GOSIP) will be best able to adapt to change. This is particularly important when the length of the procurement process is considered. Technological advances in information systems occur so rapidly that often systems require updating soon after implementation. Therefore, compliance with open systems standards should play an important role in selecting an internet solution.

APPENDIX A: NMPC ORGANIZATION AND IRM RESPONSIBILITIES

A. INTRODUCTION.

This appendix describes the functions of each of NMPC's major departments and staff sections and in Table A-1 summarizes the IRM responsibilities of each of NMPC-16's sections.

1. Administrative Sections and Special Staff.

NMPC's staff sections (NMPC-01 through NMPC-08) perform a variety of administrative and support functions requiring basic office automation tools. NMPC-01 is the command's Administrative Office. NMPC-02, the Resource Management Office, allocates and controls internal resources. Military Correspondence and Congressional Liaison are performed by NMPC-03 and NMPC-04 sets Navy uniform policy and regulations. NMPC-05 handles all Public Affairs functions and NMPC-06 is the office of the legal counsel. NMPC-07 and NMPC-08 handle transportation and passes for official visitors.

Special staff supporting the Commander NMPC includes the executive assistant, office of the chief of staff, administrative assistant, aide, and secretary. Additional special staff include an internal review officer, deputy for equal employment opportunity, an equal opportunity advisor, and the command master chief.

2. **NMPC-2, Career Progression Department.**

This department handles reenlistments, officer resignations, and recall to active duty. It manages officer promotions/appointments as well as enlisted advancements. It's responsibilities further include retirements and fitness reporting.

3. **NMPC-3, Military Personnel Record Data Management Department.**

NMPC-3 administers the micrographic information systems used to record personnel data into official service records. It controls records and personnel evaluations and provides promotion selection board services.

4. **NMPC-4, Distribution Department.**

This department matches individual personnel to duty assignments worldwide. It has the Navy's "detailers" who manage officer/enlisted assignments, allocations, and strength projections. It also administers enlisted classification and incentives programs.

5. **NMPC-5, Occupational Systems Department.**

NMPC-5 is responsible for determining the enlisted rating structure, developing and assigning enlisted classification codes, and administering the Naval Officer Occupational Class System (NOOCS). It manages the specialty designator system, to include the NOBS/subspecialties.

6. **NMPC-6, Human Resources Management Department.**

This department's major responsibilities include: health care and CHAMPUS; equal opportunity, leadership, and command effectiveness programs;

drug and alcohol abuse prevention and control initiatives; family support and housing programs; and health and physical readiness issues.

7. **NMPC-7, Military Personnel Navy Financial Management Department.**

This office performs budgeting, accounting, and programming support for funding appropriations: MPN, RPN, and RPD. It also administers PCS and various other appropriations.

8. **NMPC-8, Military Personnel Performance and Security Department.**

NMPC-8 handles matters of officer/enlisted performance and discipline, manages personnel security, and overseas corrections and deserter programs.

9. **NMPC-9, Naval Reserve Personnel Management Department.**

This department handles personnel matters for all naval reserve members to include appointments, assignments, promotions, advancements, retirements, and similar matters.

10. **NMPC-11, Recreational Services Department.**

NMPC-11 manages the Navy's Manpower Program, childcare services, and family and shipboard recreation programs. It administers mess and package store activities and handles matters concerning non-appropriated fund personnel/insurance.

11. **NMPC-12, Community and Personnel Service Department.**

This office administers benefits eligibility, casualty assistance, and voting assistance programs. It is responsible for the Navy Relief Society as well as management of the Navy Retired Affairs Program.

12. NMPC-16, Total Force Information Systems Management Department.

NMPC-16 is responsible for all facets of NMPC's internal information systems planning and management including ADP security, information resource management, data administration, life cycle management, quality assurance, systems architecture, and ADP resource allocation functions. Table A-1 on the following page summarizes NMPC-16's IRM responsibilities by section.

Table A-1: Summary of NMPC IRM Responsibilities

NMPC OFFICE	IRM RESPONSIBILITIES
NMPC-16 (OP-16)	- OPNAV staff responsibility for the Navy's MPT IRM program management. - CNP staff responsibility for MAPTIS programs. - IRM planning & management; develops & oversees implementation of CNP CIRMP.
Director, N-16	- Director, OP-16; performs OPNAV IRM management. - Performs CNP IRM staff functions. - Administers IRM activities of NMPC-16.
Deputy Dir, N-16	- Assists Director, N-16 in OPNAV, CNP, and NMPC IRM roles.
NMPC-16D	- Manages IRM personnel assignments and training.
NMPC-16E	- Manages DOD's Realtime Automated Personnel Identification System (RAPIDS).
NMPC-16F	- Information Planning and Management Office - Administers CNP IRM, lifecycle management, data management & policy making.
NMPC-16R	- Information Systems Resource Management Office - Manages planning, programming, budgeting, and execution of NMPC's IRM plans.
NMPC-163	- Customer Support Division - Plans, specifies, and implements information systems in response to requirements of NMPC line managers. - Manages contracting, installation, & training for departmental OAN's/LAN's. - Specifies, selects, and manages contracting, installation, and training of internetworking resources and personnel.
NMPC-164	- Data Management Division - Defines data requirements to meet OPNAV, CNP, and NMPC business needs.
NMPC-165	- Corporate Data Systems Division - Manages development of centralized corporate databases for Navy-wide civilian and military manpower management for DOD, DON, & higher.
NMPC-166	- Field Personnel Systems Division - Conducts planning, design, development, implementation, and maintenance of Navy-wide MPT information systems including pay system interfaces and and field office headquarter MIS.
NMPC-167	- Technology Support Division - Handles design, planning, implementation, operation, integration, and maintenance of processing & telecommunication resources. - Develops and administers CNP TAP.

APPENDIX B: LOCAL AREA NETWORKS[21]

A. WHAT IS A LOCAL AREA NETWORK?

A network is a collection of devices interconnected through telecommunications in order to accomplish the sharing of data and information processing resources. Computer networks are in widespread use and range in scope from limited nets connecting a few devices in a single location to sophisticated worldwide networks interconnecting thousands of devices.

Local area networks (LAN's) are one particular type of computer network. A LAN is normally owned by the organization in which it resides, managed by its users, and not subject to FCC regulation [Ref. 27]. LAN's are distinguished from other networks primarily by their "local" geographical scope; thus, the term "local area network" generally means a network confined to a single building or in some cases a series of buildings clustered within a couple of miles of each other. This is in contrast to networks which are dispersed over greater distances which may be called metropolitan area networks when covering a single urban area or wide area networks (WAN's) when covering larger areas.

[21]This discussion of the basic elements of a network is an synthesis of general network knowledge adapted from References 2, 14, 24, 25, 26, and 27.

B. CHOOSING THE RIGHT LAN.

Building a LAN involves the interconnection of workstations, microcomputers or other devices using some form of continuous structural medium such as coaxial cable, twisted-pair wire or optical fiber. This connectivity allows every station the ability to communicate with every other station and share resources such as peripherals, data, and application programs. Although local area networks are commercially available, installing a LAN is far from a trivial matter. LAN's require on-site engineering and a great deal of vendor interaction to ensure proper configuration, installation, and performance requirements are met. Nevertheless, the potential for reduced operational costs by sharing resources and increased productivity from improved intra-organization communications often justifies the cost of implementing a LAN.

Although all LAN's are similar in that they are composed of information processing devices interconnected by some means of telecommunication, not all LAN's are alike. They vary significantly in their exact structure and capability. Which type of LAN should be used in a given situation depends on the functional requirements of the user organization. In designing a LAN one must consider factors such as the types of data to be transmitted, volume of communications, frequency of net access, number of devices to support, geographical area, security, anticipated growth, and applications to be performed on the net. Choosing an appropriate LAN often involves tradeoffs between competing technical capabilities and requires the prioritization of desired functionality.

System planners must thoroughly understand both the business functions the net is to perform and the technical aspects of network design if they are to select the most effective LAN configuration. There are so many possible combinations of commercially available devices that this may first appear to be an overwhelming task. The key to making good network design decisions is an understanding of the basic elements of a LAN.

C. ELEMENTS OF A LAN.

There are three primary factors that determine the type of local area network: topology, transmission medium, and medium access control. In simple terms, topology is how the net is laid out -- the pattern by which its devices are interconnected. The transmission medium is the physical means by which the devices are linked -- wire, cable, optical fiber, etc. Medium access control is the method used to manage how stations access and use the net to talk to each other. In designing a LAN there are many options for each of these factors but since they are closely interrelated, making a choice in one area affects each of the others. Specifically, the topology and transmission medium determine the type of data that can be transmitted over the network, the data rate and efficiency of that transmission, and the applications that can be supported by it. Similarly, the method of access control is primarily driven by the topology and medium used. Each of these elements is discussed below.

1. **Transmission Media.**

The most basic part of a LAN's structure is the nature of the physical link used to connect its devices. In order for a network to share its resources, individual workstations must be connected with some type of transmission medium or cabling. A particular LAN application will be best served by one type cabling or another. Additionally, the transmission methods used in a net are directly related to the physical medium employed and determine the type and volume of data that may be communicated across the network.

Three types of media are currently in common use to connect devices in a LAN: twisted-pair wire, coaxial cable, and optical fiber. (Table B-1, at the end of this appendix, compares these transmission media.)

a. Twisted Pair Wire. Twisted-pair is the most readily available medium for LAN installations. Not only is it the easiest to install, but it is also the least expensive medium as it is basically the same wiring used in today's telephone systems. Twisted pair is lightweight and easily manipulated during installation. It is easy to pull through a building's walls, ceilings, floors, etc. and requires less space than other mediums. This makes it well suited to installation in existing structures. For low-traffic environments of organizations occupying a small area, twisted-pair is the most cost-effective choice. Although it is relatively inexpensive, twisted pair has some limitations in the form of lower traffic capacity, limited distance, and greater vulnerability to noise interference than other mediums.

As the name implies, twisted-pair is characterized by two insulated wires twisted together. Two wires are used to allow full duplex data transmission (simultaneous two-way communication). Twisting the wires reduces their susceptibility to electrical interference of induced currents; however, it is only somewhat reduced -- not eliminated. This noise increases as traffic does and thus increases in the data rate raise the probability of a garbled transmission and greatly reduce the rate at which data can be successfully transferred across the wire.

Twisted pair is also highly susceptible to spurious environmental noise common to office environments. Electrical wiring, office equipment, radios, and the like all produce electromagnetic interference which may disrupt twisted pair circuits. Shielding the wire through the use of increased insulating materials improves its performance by reducing its exposure to environmental noise. However, such shielding increases its cost and makes twisted pair less easy to install.

Another drawback of twisted pair, is the limited area it can cover. The distance that a data signal can travel over twisted-pair is limited by signal attenuation. As a signal travels further from its source, it attenuates or gets weaker and more environmental noise is picked up since the wire acts as an antenna. As the signal gets weaker and noise increases, effective data transmission erodes. One means of overcoming this problem is through the use of devices to boost signal strength. Such devices, called repeaters, increase the

distance which a twisted pair net can cover. Although repeaters can increase the distance of effective communications, they are expensive and their cost should be carefully considered when designing a LAN.

b. Coaxial Cable. Coaxial cable is a second, more complex physical transmission medium. It is composed of a central conductor that is surrounded by a nonconducting insulator enclosed by a shielding that acts as a ground. An insulating outer coating completes the cable. This complex composition makes the cable fairly immune to electrical interference; therefore, it can carry data at much higher rates and greater distances than twisted-pair. Coaxial cable is more expensive and slightly more difficult to install than twisted-pair. It is the same type of cable as used in cable television systems. Significant increases in data-rate, distance, and the number of workstations supported make it the choice of large LAN applications.

Two types of transmission technologies are supported by coaxial cable: baseband and broadband. They differ in that baseband transmission uses one channel to send a single signal while broadband uses multiple channels allowing the simultaneous transmission of several signals. Both have many advantages over twisted-pair wiring and meet high performance requirements, but serve different LAN applications.

Baseband is only capable of transmitting one signal at a time. Bidirectional signals are transmitted digitally at rates from 1M to 10M bps. This type of coaxial cable is easy to install and requires very little maintenance.

Taps are easy to attach to the cable and workstations can be added or removed without interrupting network operations. However, there are a few disadvantages associated with baseband coax. The area covered by a baseband LAN is usually limited to a single building. Without expensive digital repeaters, the distance that baseband can travel is limited to a few kilometers. In some areas fire regulations require that the cable be run through hard conduit, thus adding to installation costs. Finally, the limited capacity, one channel, may be too restrictive for some LAN requirements.

Broadband can transmit several signals simultaneously using different frequencies. Multiple channels (commonly 20 to 30 frequencies) are available on a single cable increasing the capacity of data that can be carried. Broadband signals are capable of traveling many kilometers through the use of inexpensive amplifiers. The analog signals used in broadband transmissions are unidirectional but can carry integrated voice, video, and data transmissions. Bi-directional communications is accomplished by using paired cables connected with a headend device.

Broadband installation is complex and requires trained technicians for the design and maintenance of the network. Broadband requires RF modems and specific channel frequencies must be carefully tuned. There are more cable and hardware requirements as well. All this adds up to a more costly LAN best suited for large configurations with tremendous capacity needs.

c. Optical Fiber. Optical fiber is the newest medium and has great potential. It differs significantly from coaxial and twisted pair mediums in that it transmits data in the light range of the electromagnetic spectrum. High speed and large capacity make it a promising medium; however, high costs and technical limitations currently keep it from widespread use. Nevertheless, optical fiber will undoubtedly become a more practical means of LAN implementation as technological developments reduce its cost. Even today, its unique advantages make it practical for some applications.

Optical fiber is impervious to corrosion and consists of a glass fiber core protected by a sturdy covering. Fiber optic cable is immune to electrical interference and capable of very high speed, high capacity signal transmissions. By using optical repeaters to amplify the signal along the way, it is possible to transmit signals several miles without experiencing any signal loss. A unidirectional signal (light beam) is sent through the fiber core of the cable by a laser or light-emitting diode (LED). Data transmission rates of up to 1 gigabit per second have been achieved. With an additional fiber in the cable, bidirectional transmissions are also possible.

The major disadvantage of optical fiber as a medium for local area networks is the difficulty of tapping into the cable. It cannot be simply cut and spliced like other mediums; therefore, connecting additional workstations to an existing network is very difficult and expensive requiring specialized hardware and net downtime. However, this disadvantage is exactly what makes optical

fiber desirable for some applications. Since the cable cannot be cut and tapped as can other mediums, it is ideal for uses where access restriction is critical. Often it is the requirement for a secure network, free from electrical interference, which outweighs the increased cost of optical fiber and makes it the most appealing medium in some circumstances.

2. Topology.

The layout of a network, the pattern in which the devices of a LAN are interconnected by physical links, is called its topology. There are three basic LAN topologies: bus, ring, and star. They are characterized by the physical configuration of a LAN's workstations in relation to one another. Each topology has unique advantages and disadvantages. Several factors should be taken into consideration when selecting an appropriate LAN topology. Among these are the data rate required, the maximum number of stations to be supported, the maximum operating distance to cover, and total system costs. (Table B-2, at the end of this appendix, compares the network topologies discussed below.)

a. Bus Topology. The most common type of LAN configuration is a bus topology using coaxial cable (Figure B-1). This topology uses a linear transmission medium shared by network devices attached directly to it. The single transmission medium of a bus makes it easy to add or remove workstations when required provided a minimum distance between taps on the bus is maintained to prevent signal interference. Bus's are fairly reliable in that

the failure of a station will not disable the entire network, while a break in the cable may only affect part of it.

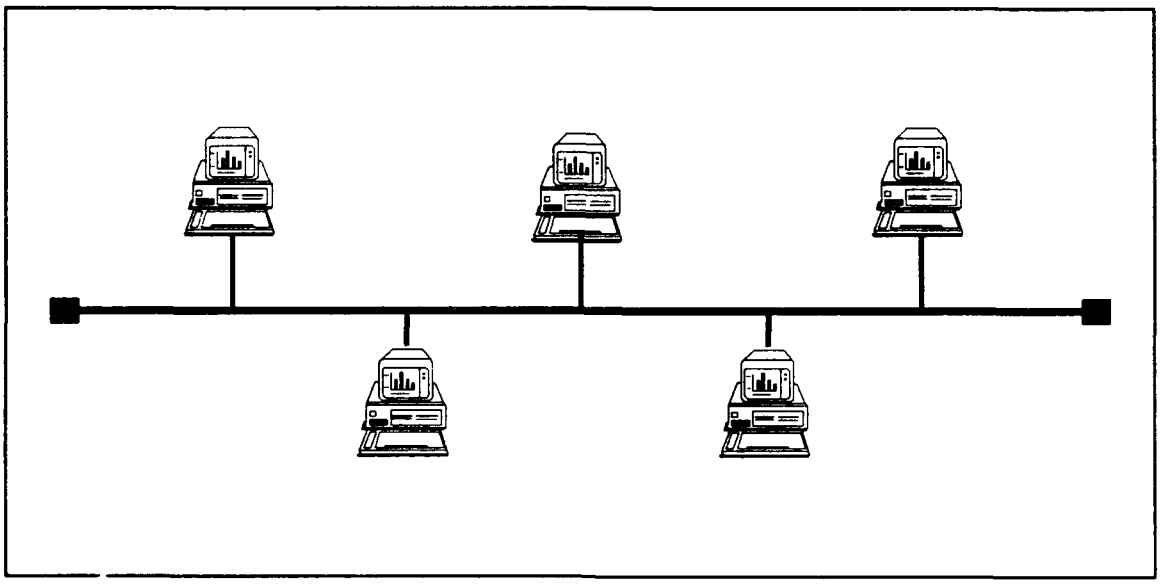


Figure B-1: Bus Topology

Transmissions across a bus are broadcast to all stations. Since all transmissions pass every station, each must check every transmission to determine if it is meant for it or not. Each station may communicate with every other station with access to the bus being managed by some means of medium access control as discussed in paragraph 3 below.

Bus topology networks suffer minor drawbacks in the areas of security and maintenance. It is very difficult to maintain security since all transmissions travel across a common data path. An unauthorized user on a bus has the potential of intercepting any transmissions on the net. Maintenance is also troublesome since running network diagnostics is difficult on a bus. Nevertheless, potentially high data transfer rates and the ability to

accommodate a large number of stations outweigh the disadvantages of a bus for most organizations.

All broadband networks, and many baseband networks, use bus topologies. Low-cost LAN's often use a bus built with twisted-pair wiring provided a great deal of speed is not required. If greater capacity and higher performance is desired, coaxial cable, or even optical fiber can be used. The increase in capability will, of course, increase the cost of the network.

b. Ring Topology. A ring topology consists of several repeaters connected to each other with unidirectional transmission links to form a single closed loop (Figure B-2 on following page). Repeaters serve as an attachment point for each workstation to the network. The workstations are arranged along the transmission path so that a signal must pass through every station one at a time around the entire loop until it returns to the station originating the signal. Ring topology networks may be built using twisted-pair, baseband coaxial cable, or optical fiber. One station normally exercises master control of this type of network in a manner transparent to the user.

Signal transmission is achieved by a sequential, bit-by-bit data transfer around the loop in one direction. All messages pass every station. A method of message verification is employed so that the originating station can be assured that the designated station received the message. In a ring topology, repeaters are responsible for the insertion, reception, and removal of data from the network. A repeater failure or a break in the loop can disable the entire

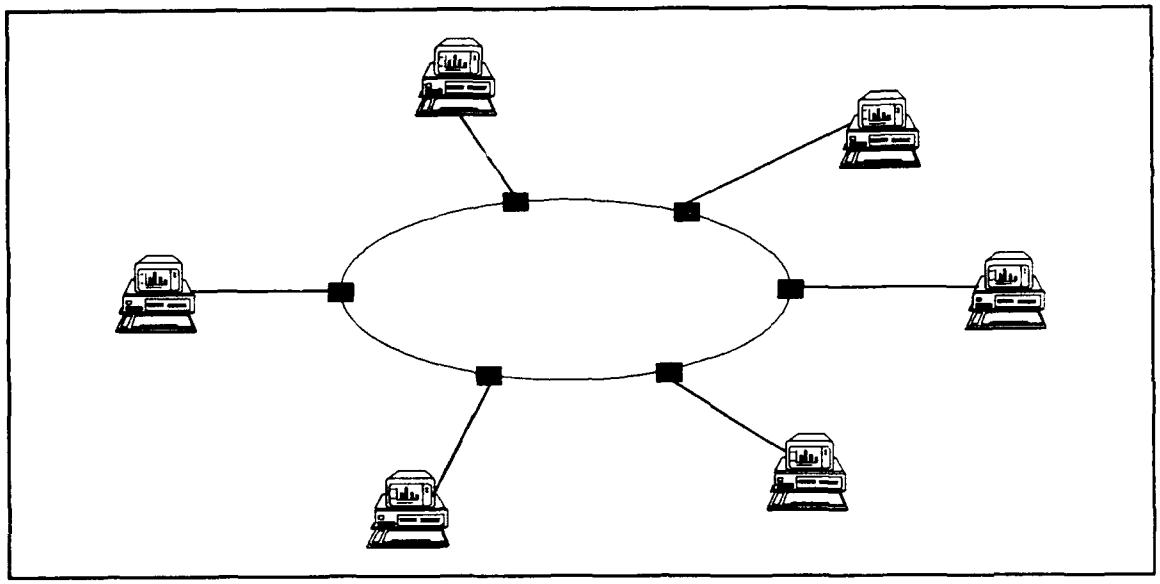


Figure B-2: Ring Topology

network unless some sort of bypass circuitry has been implemented. A dual ring configuration is often used to provide such circuit redundancy.

*c. **Star Topology.*** The star topology is much like a central-switching phone system. Each station is connected to a central computer by a single point-to-point link (Figure B-3).

This configuration makes it easy to add new workstations to the network. There are few hardware requirements involved. Simply attach a cable from the central computer to the workstation's network interface card. The central computer processes all of the workstations requirements so centralized diagnostics of all of the networks functions are possible. The dependency on the central computer is also the major weakness of the star topology. Although the failure of one station will not effect the rest of the net; if there are any problems with the central computer, the entire network is disrupted.

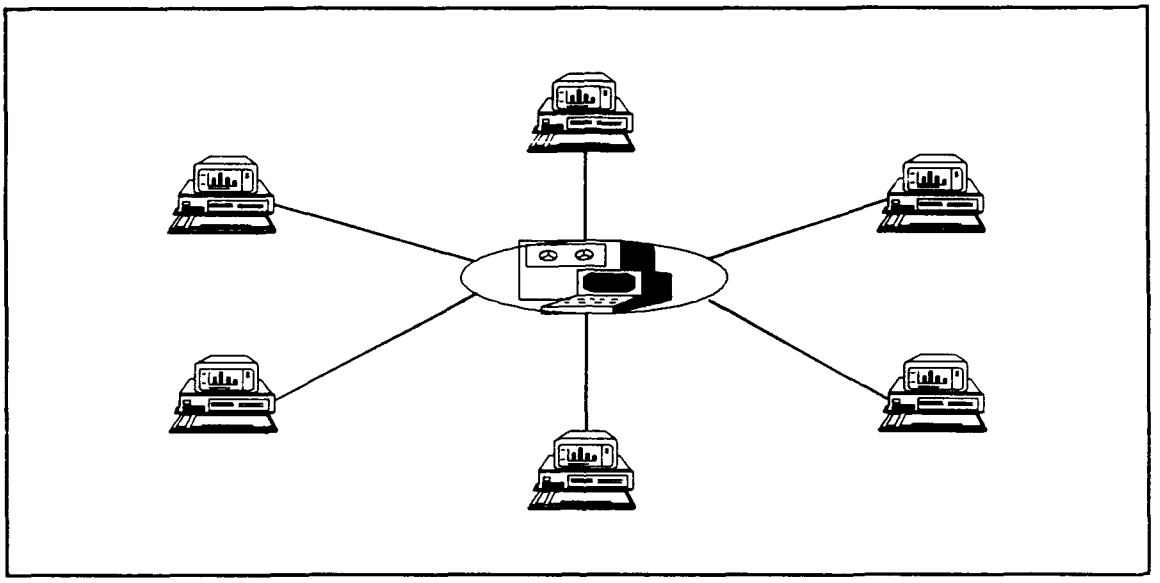


Figure B-3: Star Topology

3. Medium Access Control Methods.

All stations on a LAN share a common medium so only one station can transmit at a time. Therefore, a method of controlling and distributing the right to transmit on the network is necessary. Distributed access methods are most often used allowing all stations of the network to equally participate in its control. There are two classes of distributed access control: random or "contention" and deterministic. These are distinguished by the method a station employs in order to initiate a transmission.

Contention methods allow any station on the network to initiate a transmission at any time. Carrier Sense, Multiple Access with Collision Detection (CSMA/CD) is the most common contention method of medium access. Bus topology networks often use CSMA/CD. It is a method based on detecting and avoiding data collisions. All stations listen to the transmission

medium prior to and during a signal transmission. If traffic is sensed on the medium, any station that wants to transmit waits a random interval, listens again and then transmits if no traffic is sensed. Similarly, when a collision is detected, the station retransmits after a random interval. CSMA/CD works well for LAN's that have long, infrequent messages rather than several, small messages. As the number of workstations and medium length increase on a network, the number of collisions will increase and result in a substantial decrease in the total performance of the network.

Deterministic methods require that stations take turns transmitting in accordance with specified rules. Each must wait for its turn to transmit. This is normally done through a token passing method. The possession of a "token" by a station indicates transmission authorization. Token Bus and Token Ring are the most common deterministic access methods.

Token Bus is the most widely used deterministic method of access control. Token bus networks experience better performance under heavy traffic than CSMA/CD networks. The transmission of data is possible only if the station is in possession of the token. Workstations on the bus circulate a token (a special bit pattern) around a logical ring. The physical configuration of the bus is irrelevant to the logical order for passing the token. The right to transmit is determined by possession of the token. The station with the token is granted control of the medium for a specified amount of time to transmit. The station receiving the message, copies it and then returns the token to the

originating station. When a station's transmission is complete or its time has expired, it then passes the token to the next workstation in the logical sequence. Although token passing reduces the possibility of collision between transmissions, token schemes require more complex network management. As a result, token bus networks require more maintenance than contention managed buses. Whenever a token bus network is started up or the logical ring breaks down, the network must go through a re-initialization process.

Token Ring is another deterministic method of access control that is regulated by the possession of the token. The token is circulated around a physical and a logical ring. The station initiating the transmission attaches its message to the token and circulates it around the ring until it is received and copied by the addressed station. The token is designed to inform the originating station if the message was properly received and copied by the intended station. After the token is returned to the originating station and a successful transmission has been completed, the token is passed to the next station. Each station on a token ring network repeats the signal as it passes so it is possible to cover a greater distance than a token bus network without signal loss. Amplifiers can also be used to boost the signal.

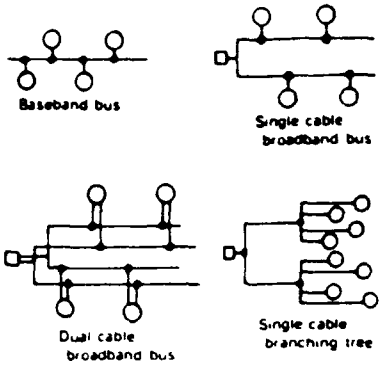
Deterministic methods of medium access control (e.g. token bus and token ring) have some advantages over contention systems. Under token passing, the possibility of a collision is effectively eliminated resulting in steady-state operation. Token systems may incorporate timing mechanisms to

establish predictable times in which given stations may expect to gain access to the net. This differs from contention schemes in which high volumes of traffic may cause degeneration of the net into chaos with unpredictable access times. These advantages come at a higher cost than contention management methods since they are more complex to implement. It is more difficult to design deterministic networks due to the additional considerations involved with logical addressing and sequencing. Under token passing schemes methods of prioritizing a station's access to the token, may be used to give better access to critical stations if desired. Token passing schemes require more data overhead in each transmission and add to the complexity of net management.

TABLE B-1: Comparison of Transmission Media *(Source: DataPro, March 1988)*

	Twisted-pair wire	Baseband coaxial cable	Broadband coaxial cable	Fiber optic cable
Topologies supported	Ring, star, bus, tree	Bus, tree, ring	Bus, tree	Ring, star, tree
Maximum number of nodes per network	Generally, up to 1,024	Generally, up to 1,024	Up to about 25,000	Generally, up to 1,024
Type of signal	Single-channel, unidirectional; analog or digital, depending on type of modultaion used; half- or full-duplex	Single-channel, bidirectional, digital, half-duplex	Multichannel, unidirectional, RF analog, half-duplex (full-duplex can be achieved by using two channels)	One single-channel, unidirectional, or bidirectional simultaneously over a single wavelength half- or full-duplex, signal-encoded light-beam per fiber; single-encoded lightbeam per fiber; single fiber per cable
Maximum bandwidth	Generally, up to 4M bps (or higher)	Generally, up to 10M bps	Up to 400MHz (aggregate total)	Up to 200M bps in 10-kilometer range; up to 1G bps in experimental tests
Major advantages	Low cost May be in existing plant; no rewiring needed, very easy to install; easy to support	Low maintenance cost Simple to install and tap	Supports voice, data, and video applications simultaneously Better immunity to noise and interference than baseband More flexible topology (branching tree) Rugged, durable equipment; needs no conduit Tolerates 100% bandwidth loading Uses off-the-shelf, industry-standard CATV components	Supports voice, data, and video applications simultaneously Immunity to noise, crosstalk, and electrical interference Very high bandwidth Highly secure Low signal loss Low weight/diameter; extremely flexible, pliable; can be installed in small spaces Durable under adverse temperature, chemical, and radiation conditions
Major disadvantages	High error rates at higher speeds Low immunity to noise and crosstalk Lacks physical ruggedness, requires conduits, trenches, or ducts Speed and distance limitations Existing plant may be unsuited to data transmission (i.e., wire pairs may not be twisted, grade and quality may vary, accurate cable records may not be available)	Lower noise immunity than broadband (can be improved by the use of filters, special cable, and other means) Bandwidth can carry only about 40% load to remain stable Limited distance and topology Conduit required for hostile environments Not highly secure Rigid and bulky, difficult to install More expensive than twisted-pair	High maintenance cost More difficult to install and tap than baseband RF modems required at each user station; modems are expensive and limit the user device's transmission rate Rigid and bulky, difficult to install More expensive than twisted-pair	Higher cost, but declining Requires skilled installation and maintenance personnel Taps not perfected Currently limited to point-to-point connections

TABLE B-2: Comparison of Basic Topologies *(Source: Datapro, March 1988)*

Topology	Typical Schematics*	Performance Considerations	Constraint Considerations
Linear bus		Delay—in token bus networks waiting time is a fixed function dependent on number of nodes in network. in contention bus networks delay is a variable dependent on current traffic. delay distortion (jitter) is possible Throughput—in token bus networks. throughput decreases with each node added. in contention networks. throughput is best in light bursty traffic conditions. and decreases in high volume steady traffic environments Reliability—failure of one station will not affect the rest of the network. break in cable may affect only part of the network Robustness - relationship between stations is peer to peer. network is difficult to monitor in contention networks the difference between noise and collisions may be difficult to distinguish	Circuit speed—varies up to 50M bps Distance—generally unlimited by topology Maximum number of nodes—user stations may be added or deleted without reconfiguring the networks. in token bus networks addition of each station directly affects performance Error rate—bit errors are lowest when fiber optic cable is transmission medium. low when coax cable is used higher with twisted pair wire Cost—generally lower cost per user station than star networks and higher than ring networks
Ring		Delay—waiting time is fixed function dependent on number of nodes in network Throughput—decreases with each added node Reliability—if one station fails whole network fails unless bypass circuitry has been implemented in each interface or node. if loop is severed the whole network fails unless redundancy features have been implemented potentially low reliability can be compensated for by high quality engineering design Robustness—Nodes are easy to understand construct and maintain may require custom-designed device dependent interface communications control overhead is generally high if network fails recovery may be difficult and may require complex logic and processing	Circuit speed—varies up to 10M bps Distance—limitations are imposed both on total distance and distance between nodes Maximum number of nodes—may be a fixed parameter dependent on command station capacity. addition of each station directly affects performance Error rate—twisted pair wire is vulnerable to transient errors fiber optics has very low error rate Cost—generally. lower cost per station than other topologies
Star		Delay—in heavy traffic conditions requests for service may be blocked at the switch in a PBX Throughput—dependent on internal bus capacity of central node Reliability—failure of one station does not affect the rest of the network if central node fails the whole network fails Robustness—Ready availability of network monitoring and control software high overhead for communications control corresponds well to applications in hierarchical (master slave) networks	Circuit speed—varies considerably depending on medium Distance—limitations are imposed on distance between central node and any user station Maximum number of nodes—expansion limitations are dependent on capacity of central node difficult to reconfigure Error rate—twisted pair wire is vulnerable to transient errors Cost—high initial cost but low incremental costs thereafter

*Schematic symbols

— Transmission medium
○ User station
● Connection device (network interface unit RF modem transceiver etc.)
□ Command station (central host PBX switch etc.) or cable head-end

APPENDIX C: INTERNATIONAL STANDARDS ORGANIZATION[22] OPEN SYSTEMS INTERCONNECTION MODEL

A. BACKGROUND.

The International Standards Organization (ISO) is a voluntary organization of representatives of the standards making bodies of participating countries [Ref. 26:p. 13]. It exists to encourage technological standardization as a means of best serving the collective interests of public and private sector producers and users of technology. With the proliferation of information systems, ISO recognized the need to produce network communications standards to ensure the compatibility of diverse vendors' products. In 1977, it established a subcommittee to develop a theoretical framework for the definition of network communications requirements. The ISO Standard Reference Model for Open Systems Interconnection (OSI model) is the framework the committee developed and ISO adopted in 1983. Since its development, the OSI model has gained widespread acceptance in both the US and abroad. In fact, it is now acknowledged to be a benchmark standard which vendors must accommodate if they are to remain competitive.

[22]This discussion of the OSI model is synthesis of general knowledge adapted from References 3, 11, 14, 15, 25, and 26.

B. NATURE OF THE OSI MODEL.

The OSI model is a theoretical framework that defines the standards necessary to ensure communications compatibility of heterogeneous computers. Its principal purpose is to provide a common basis for the design and implementation of network architectures. Its guidelines are intended to foster the development of "open systems", which can be easily interconnected and facilitate distributed processing. ISO defines an open system as one that conforms to the OSI model and its associated standards for communications interconnectivity. Conformity to the model ensures the capability of effective information flow among systems while allowing some variations of the basic communications technology employed.

The OSI model does not prescribe specific standard protocols. Rather, it is a common theoretical framework that categorizes complex networking problems into subdivisions of related functions known as layers. The model divides communications architecture design problems into seven layers as shown in Figure C-1 and thus provides a logical decomposition of the complex problems associated with interconnection requirements of a network. The seven-layer approach to standardization partitions and groups into more comprehensible parts the functions necessary for communications between computers. This allows system architects to address limited aspects of networking problems layer by layer thus facilitating their conceptualization and solution. Adherence to

the standards defined by these seven layers, ensures that diverse devices will have the ability to communicate effectively.

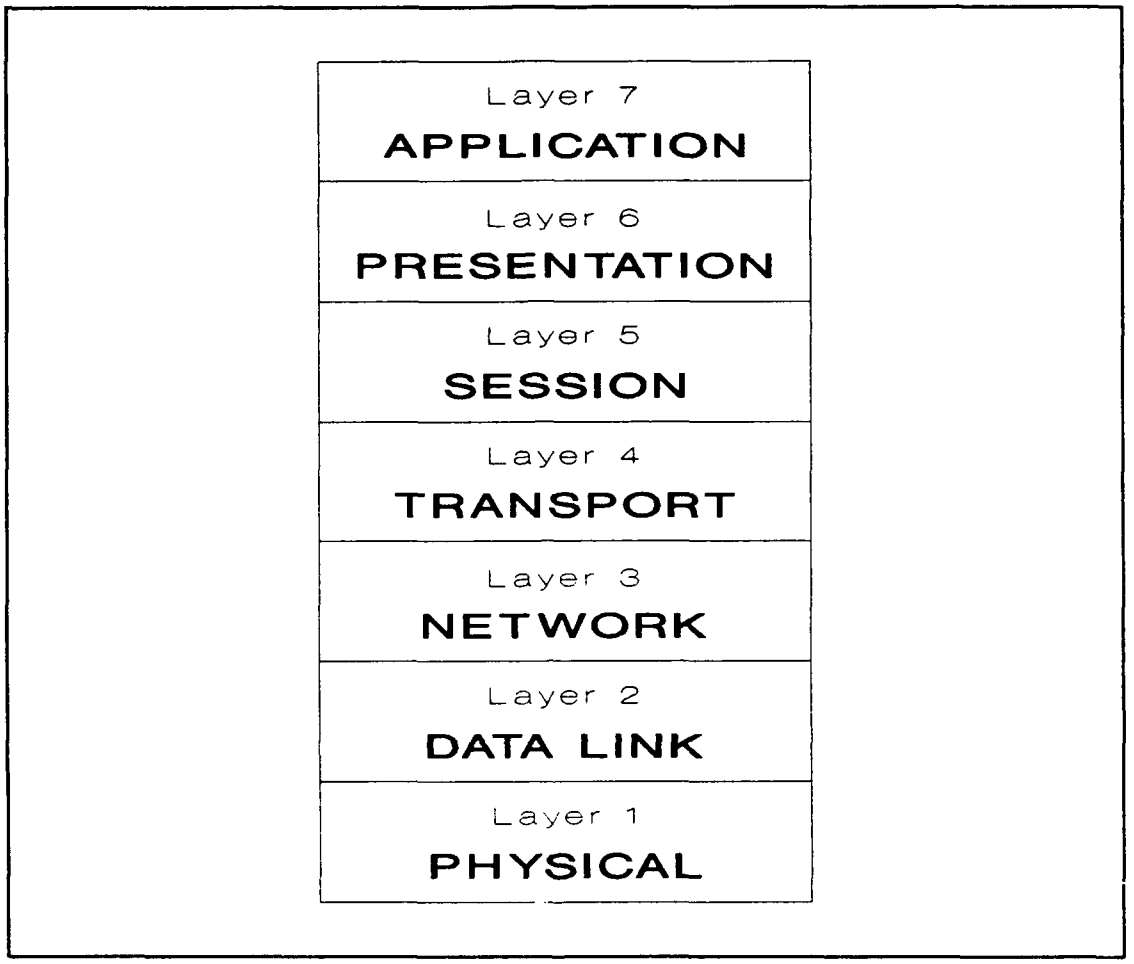


Figure C-1: Seven Layers of the OSI Reference Model

The layers of the model are closely related. Each supports or provides designated services for the next higher layer. The partitioning of functions into separate layers allows changes to be made internally to one layer without necessarily requiring changes in other layers. Each higher layer in the model incorporates aspects of the subordinate layers. For example, Layer 7, the application layer, provides the user with all of the services of the lower layers.

C. LAYERS OF THE OSI MODEL.

Figure C-1 shows the seven layers of the OSI model: Physical, Data, Network, Transport, Session, Presentation, and Application. The model defines the communications functions and services to be provided by each layer but not how those functions and services are to be performed. This gives systems designers flexibility in the technical implementation of the model's requirements.

1. Physical Layer.

The first layer is concerned with the actual physical interface between the devices on the network. It is also a set of rules regarding the transfer of unstructured data bits over a physical medium. These rules cover four characteristics of accessing the medium: electrical, mechanical, functional, and procedural. They describe acceptable connector characteristics, specifications for the physical signal, and cabling/wiring interfaces.

2. Data Link Layer.

This layer assembles bits of a data stream into packets to be transmitted over the medium by adding physical addressing information and mathematical error checking data [Ref. 15:p.125]. The rules prescribed in this layer provide guidelines for link reliability, synchronization of data from the physical layer, and error and flow control. Mechanisms to recover from lost, duplicated, or erroneous data allow the next higher layer to expect an error-free transmission.

3. Network Layer.

This layer determines the path packets take as they are transferred through the network, based on destination and routing information contained within the packets. It also accommodates special messages used in internetworking by devices such as routers or gateways in exchanging descriptions of networks among themselves. The network layer also provides special services that manage the translation between logical and physical network naming conventions. [Ref. 15:p. 125] This layer allows for the transparent transfer of data between transport layer protocols. It establishes, maintains, and terminates communications connections and is concerned with packet switching, network routing, and flow control between nodes.

4. Transport Layer.

The transport layer governs the integrity and delivery of data through the use of error-checking, sequencing methods, and other techniques which act together to ensure effective, correct transmission of logical messages. This layer maps a collection of physical messages capable of being transmitted with an overall logical message which may be too large to send as a single physical message. The transport layer divides oversized messages into packets for transmission and handles their reassembly and resequencing upon receipt at their destination. [Ref. 15:p. 125] In other words, the transport layer provides a transparent, reliable mechanism for the transfer of data between end points. It has extensive error detection and recovery capability to compensate in the

event of unreliable network layer services. The transport layer is concerned with optimization and quality of network services. The guidelines which govern this layer are designed for the effective multiplexing of messages and efficient regulation of information flow. The functions performed at this layer help isolate the user from the physical and functional aspects of network.

5. Session Layer.

This layer governs the initiation and termination of a communication session between nodes. [Ref. 3:p. 123] It provides control structures to establish, manage, and terminate the exchange of data between two or more connections. Once a communications session has been established, this layer synchronizes and manages communications which may be two-way simultaneous, two-way alternating, or one-way dialogues. Rules at this level provide procedures and sequences for reestablished disrupted communications links in the event of some failure. Users directly interact with the transport layer as it functions to perform network management, logon-logoff procedures, and password control.

6. Presentation Layer.

This layer is concerned with "presenting" data in an appropriate form to a using system or program. It is concerned with the syntax of data for use by application processes and works to resolve differences in data representation and format. The presentation layer provides services including data coding,

compression, and encryption as well as protocol conversion and translation. Network security and file transfers are also handled by this layer.

7. Application Layer.

This is the layer which performs the remaining controls necessary for higher level application processing to occur [Ref. 3:p. 123]. Application specific password controls, error recovery, and synchronization requirements are also addressed at this level. The application layer supports advanced network management functions and distributed applications such as e-mail and file server programs.

D. APPLYING THE OSI MODEL.

The OSI model allows systems architects to subdivide and logically separate the activities necessary for achieving effective networked communications. It allows the isolation and solution of complex problems inherent in providing workable network services through a "divide and conquer" approach. In this way, the model lets designers and developers segregate networking activities into an ordered hierarchy of tasks which can be handled individually while ensuring their ability to work together as part of a comprehensive system. [Ref. 15:p. 125]

The goal of ISO's model is to encourage the development of open systems which facilitate the communication of data between heterogeneous network devices. In this context, an "open" system is one that conforms to the standards for connection prescribed by the OSI reference model. The standardization of

functions and division of complex communications procedures into a set of generally accepted conventions permit different systems to communicate effectively with each other. The operation of any new network is made easier and less expensive by adhering to the standards defined by the OSI reference model. For this reason, the model has been accepted by government and private sector organizations as the best standard by which to design and implement effective information systems networks.

APPENDIX D: IEEE STANDARDS

A. BACKGROUND.

The Institute of Electrical and Electronics Engineers (IEEE) is a professional society which promulgates standardization guidelines for electronic and information processing equipment. To facilitate its work in the area of data communications, it established a committee to develop standards for Local Area Networks based on the ISO/OSI reference model. The intended purpose of these standards is to ensure the network compatibility of equipment from a variety of manufacturers. The guidelines the committee developed are called IEEE 802, a set of proposed standards divided into six sections. Four of those sections have been approved by the IEEE Standards Board and are designated: 802.2, 802.3, 802.4, and 802.5. [Ref. 28]

With the variety of networks in use, the committee decided not to adopt a single standard but instead to adopt a set of standards covering various network architectures. The several standards which resulted from the committee's work accommodate a variety of topologies and access methods available from various manufacturers. In designing a network architecture, the optimal topology and access method are driven by the specific LAN application.

B. IEEE 802 STANDARDS.

IEEE 802 is structured around a three layer model: physical, logical link control, and medium access control. These three layers for LAN access correspond to the first two layers of the OSI reference model -- the physical and data link layers. Hardware from different manufacturers will be compatible for these layers if they conform to IEEE 802 standards. [Ref. 28]

IEEE 802.2 defines Logical Link Control (LLC), a standard which provides for the exchange of data between service access points (SAPs), and Medium Access Control (MAC) a standard concerned with data collision detection. The MAC and LLC correspond to the data link layer of the OSI model (Figure D-1).

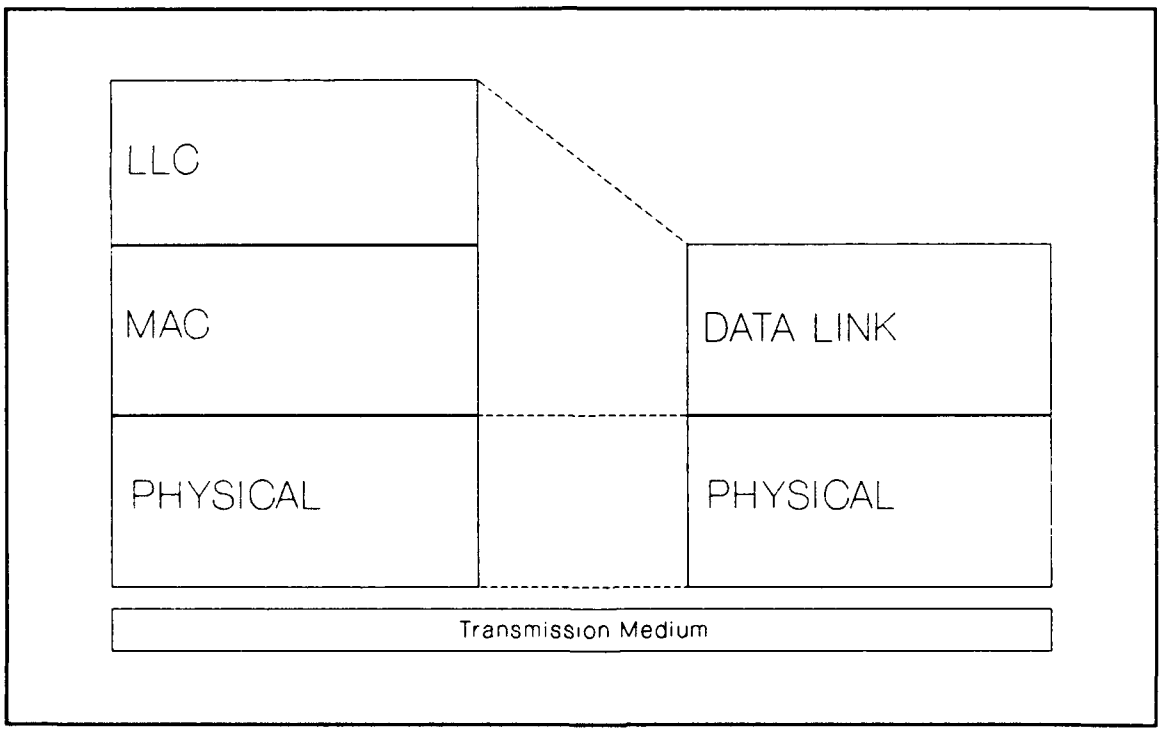


Figure D-1: Comparison of IEEE 802 and OSI Layers 1 and 2

The Logical Link Control layer provides a connectionless, datagram-like service as well as a connection-oriented, virtual-circuit-like service. The connection-oriented service provides a logical connection between SAPs, flow control, sequencing, and error recovery. The connectionless service provides for the acknowledgement of individual frames and supports end-to-end transfers. The LLC serves as a interface for a higher layer and acts to isolate the network layer from the functions of the MAC layer. [Ref. 28]

The Medium Access Control layer is concerned with the regulation or control of access so that only one device attempts to transmit at a time since a common medium is shared by several devices. The MAC has three standards that have been approved by the IEEE Standards Board. IEEE 802.3 specifies CSMA/CD as the access method for a bus topology. IEEE 802.4 uses a token passing access method on a bus topology. IEEE 802.5 specifies a token passing access method on a ring topology. [Ref. 28]

IEEE 802.3 is based largely on the Ethernet standard. It is described as a bus topology using 50-ohm coaxial baseband cable that can support a data rate of 10M bps. CSMA/CD is the method of medium access control. The physical layer of 802.3 specifies a variety of transmission medium and data rate options as shown in Table D-1 on the following page.

The IEEE 802.4 Token Bus standard is defined as a bus topology network that uses a token passing method of access control that effectively eliminates data collisions. The "Token" or data packet is required to be in the possession

Table D-1: Physical Layer Alternatives of IEEE 802.3

	10BASE5	10BASE2	1BASE5	10BROAD36
Medium:	Coaxial (50 ohm)	Coaxial (50 ohm)	Unshielded Twisted Pair	Coaxial
Signaling:	Baseband	Baseband	Baseband	Broadband
Data Rate:	10M bps	10M bps	1M bps	10M bps
Max Segment:	500 m	200 m	500 m	1800 m

of the workstation that desires to transmit a message. Since there is only one token, only one workstation is cable of transmitting at a time, thus eliminating the possibility of a collision. Token bus describes a physical bus topology that uses a logical ring addressing scheme. [Ref. 28]

IEEE 802.5 Token Ring standard is a ring topology network that uses token passing to transmit information to the workstations around a physical and a logical ring. The token is passed in much the same manner as with a Token Bus network. The major advantage of Token Ring over Token Bus is it has a greater range. Each workstation on the ring repeats the signal as it passes it on. This allows the signal to cover a greater distance without experiencing a significant loss in signal strength. The Token Ring topology is considered the best suited for large networks that cover a long distance. [Ref. 28]

The key aspects of IEEE's standards for local area networks are summarized on the following page. Figure D-2 shows the IEEE 802 standard for the first three layers of the OSI model.

Three Layer Model of IEEE 802 Standards:

1. **Physical** - concerned with the nature of the transmission medium and the physical interfaces and electrical signaling.

2. **Medium Access Control** - control access to medium so that only one device attempts to transmit at a time.

3. **Logical Link Control** - Establishes, maintains, and terminates a logical link between devices.

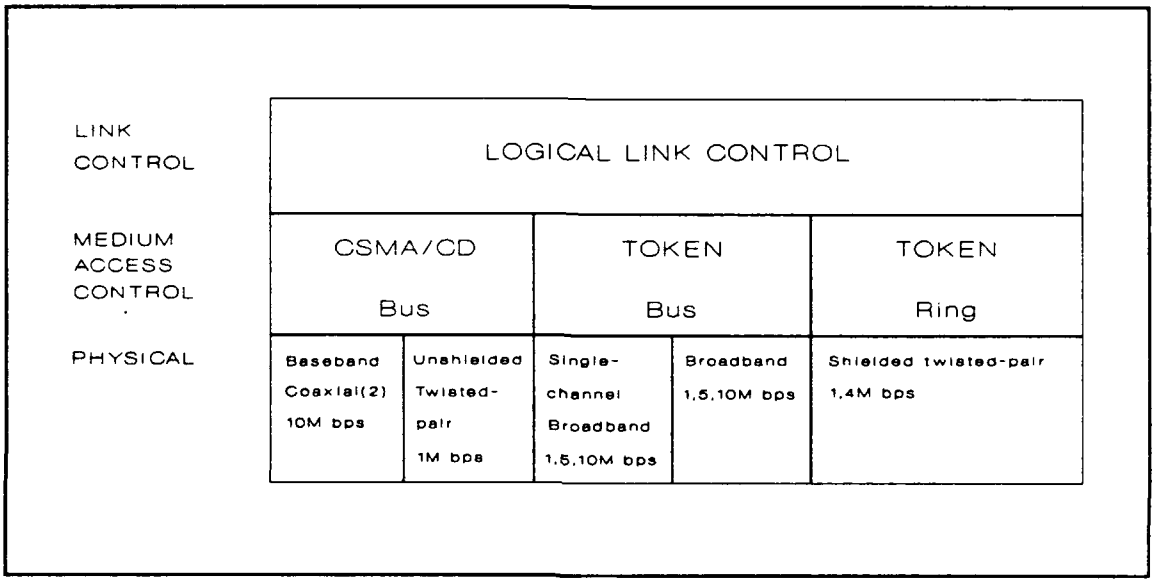


Figure D-2: Three Layers of IEEE 802

SUMMARY of IEEE 802 Standards:

802.2 Logical Link Control

802.3 1.) CSMA/CD MAC for bus topology
2.) Supports a variety of medium and data rates

802.4 1.) Token Bus MAC for bus topology
2.) Supports a variety of medium and data rates

802.5 1.) Token Ring MAC for ring topology
2.) Physical layer based on shielded twisted-pair at 1-4M bps

APPENDIX E: GOVERNMENT OPEN SYSTEMS INTERCONNECTION PROFILE

A. BACKGROUND.

Due to the incompatibility of protocols, applications, data formats, and hardware, the integration of computers from different manufacturers is a difficult task. The scope of the Government environment adds to complicate compatibility requirements. With the proliferation of diverse information processing resources and the need to exchange information between them, the United States government has recognized the need for standardization to ensure maximum potential for interoperability. Accordingly, the government now promotes the acquisition of open systems to meet information processing requirements. An open system implements common international standard communications protocols allowing interconnection with other open systems. The implementation of open systems reduces duplicate circuits and wiring, simplifies training, precludes the need for custom software, and eliminates requirements of custom work stations and hardware interfaces. Thus, the government experiences significant savings in the cost of computer systems by requiring that open systems interconnection guidelines be met.

To develop such guidelines, the National Bureau of Standards in cooperation with the information resources managers of key federal agencies established the U.S. Government Open Systems Interconnection User's Committee [GOSIP]. This

committee reviewed existing industry standards and communications protocols and developed the Government Open Systems Interconnection Profile (GOSIP) as the standards to be met in designing and procuring information processing systems. Specifically, GOSIP outlines the protocols and standards acceptable for use in government applications.

B. GOSIP COMPLIANCE REQUIREMENTS.

GOSIP defines the procurement profile for open systems computer network products. It is intended to be used by Government agencies for the acquisition of products and services. It became a Federal Information Processing Standard (FIPS Pub 146) in August 1988. In terms of enforcement, GOSIP is a voluntary, but recommended, guideline for networking procurements until August 1990. After that date, it is a mandatory standard which all procurements of new networking products and services must meet. Waivers for compliance with GOSIP can be obtained on an exception basis provided certain conditions can be met. Specifically, if compliance would effect the mission of the organization or if the financial impact of compliance is not offset by Government-wide savings, then a waiver can be granted. [Ref. 30]

C. THE NATURE OF GOSIP.

GOSIP defines a common set of data communications protocols which enable systems developed by different vendors to interoperate and enable the users of

different applications on these systems to exchange information. It addresses the need of the Federal Government to move to multi-vendor interconnectivity without sacrificing essential functionality already implemented in critical networking systems. [Ref. 17] It offers benefits to Government computer users, facilitating applications such as electronic mail, message handling, file transfer and remote file access, virtual terminal and directory services, as well as network security and management. [Ref. 29] It provides specific peer-level, process-to-process and terminal access functionality between computer system users within and across government agencies [Ref. 17]. It also includes the standards for WAN's, LAN's, and integrated voice, data, and video (ISDN). GOSIP addresses communication and interoperation among end systems and intermediate systems.

GOSIP provides implementation specifications derived from the service and protocol standards issued by the ISO, CCITT, and IEEE. It is the standard reference for all Federal Government agencies to use when acquiring and operating ADP systems or services and communication systems or services and ensure conformance to the ISO/OSI standards. GOSIP consists of a set of OSI protocols for computer networking that are intended for acquisition and use by government agencies. All federal agencies are required to apply GOSIP when acquiring products and services to ensure that all procurements provide equivalent functionality to the OSI protocols it references.

GOSIP is a dynamic profile which specifies the protocols required at each layer of the OSI Reference Model. Currently, it names a large variety of network protocols for the lower layers of the OSI model. As higher level protocols continue to evolve they will be included in subsequent releases of GOSIP. [Ref. 30] On the following page, Figure E-1 shows the standard protocols GOSIP specifies as they relate to the seven layers of the OSI Model. A list of these protocols is given on the pages following Figure E-1.

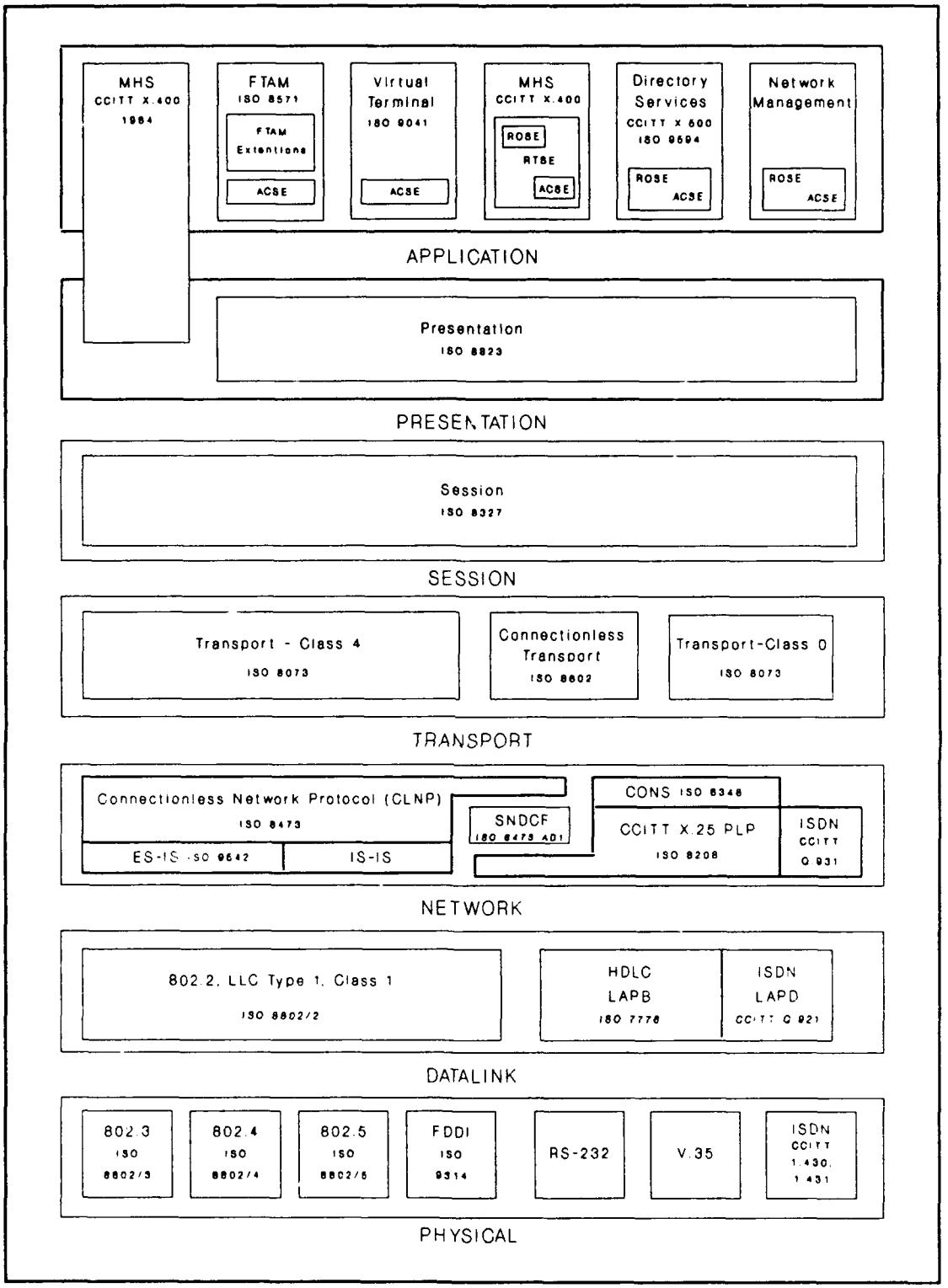


Figure E-1: GOSIP Protocols

GOSIP PROTOCOL REQUIREMENTS BY LAYER OF THE ISO/OSI MODEL

Physical Layer - In conjunction with X.25, choose between the Interim MIL-STD-188-144-A [DOD 1], and EIA-232 [EIA 1]. In conjunction with the use of IEEE 802.2 Logical Link Control Type 1, either IEEE 802.3, IEEE 802.4, or IEEE 802.5 will be used.

Data Link Layer - Selected by the Acquisition Authority, HDLC and its subset LAPB will be used in conjunction with X.25, and LLC IEEE 802.2 in conjunction with IEEE 802.3, IEEE 802.4, or IEEE 802.5.

Network Layer - The ISO connectionless internetwork protocol (IP) can be used. It must be implemented for the internetworking of concatenated networks as well as for single networks. Connection-oriented networks use X.25, while ISO 8348 and ISO 8473 are selected for connectionless networks.

Transport Layer - Transport class 4 (TP4) shall be provided by the vendor in accordance with section 4.5 of the Workshop Agreements. Transport class 0 (TP0) is to be used in conjunction with CCITT X.400 as appropriate.

Session Layer - Uses ISO IS 8326 and IS 8327 or CCITT X.215 and X.225.

Presentation Layer - Uses ISO DIS 8822, DIS 8823, DIS 8824, and DIS 8825.

Application Layer - Uses FTAM, and the X.400 Message Handling Systems set of protocols.

SPECIFIC PROTOCOLS CITED IN GOSIP

CCITT X.400 Message Handling System (X.400-1984)

ISO 8571 File Transfer, Access and Management (FTAM)

ISO 8650 Protocol Spec. For the Association Control Service Element (ACSE)

ISO 8823 Connection-Oriented Presentation Protocol (Presentation)

ISO 8827 Basic Connection-Oriented Session protocol (Session)

ISO 8073 Connection-Oriented Transport Protocol Specification Class 4 (TP4)

ISO 8473 Protocol for providing Connectionless-mode Network Service (CLNP)

CCITT X.25 and ISO 8208 X.25 Packet Level Protocol for Data Terminal Equipment (X.25 PLP)

ISO 8802-2 Logical Link Control Type 1 (LLC1)

CCITT X.25 and ISO 7776 Description of the X.25 LAPB-Compatible DTE Data Link Procedures (X.25 LAPB)

ISO 8802-3 Carrier Sense Multiple Access with Collision Detection Access Method (CSMA/CD MAC)

ISO 8802-3 Carrier Sense Multiple Access with Collision Detection Physical Layer Specification (CSMA/CD 10BASE5)

DIS 8802-4 Token-Passing Bus Access Method Specification (Token Bus MAC)

DIS 8802-4 Token-Passing Bus Physical Layer Specification (Token Bus PHY)

DIS 8802-5 Token Ring Access Method Specification (Token Ring MAC)

CCITT V.35 Data Transmission at 48K bps using 60-108 kHz Group Band Circuits (V.35)

EIA RS-232-C Interface between DTE and DCTE employing Serial Binary Data Interchange (RS-232-C)

APPENDIX F: BUILDING AN INTERNET

A. INTRODUCTION.

The purpose of this appendix is to familiarize the reader with general technical aspects of bridges and gateways -- the two principal means by which local area networks may be interconnected to form an internet.[23] It is written with the assumption that the reader has a working knowledge of the characteristics of local area networks and an understanding of the layered functions of the OSI model and associated networking standards. Readers who are unfamiliar with these areas should read Appendices B through E before continuing. The overall goal of the chapter is to give the reader sufficient technical familiarity with bridges and gateways to understand the discussion of NMPC-specific connectivity requirements presented in Chapters 7 and 8.

B. CONNECTING NETWORKS.

In connecting networks, provisions must be made to handle a variety of tasks. The connection must provide a link which allows for routing and delivery of data between networks and in doing so reconcile any differences which may exist in the addressing schemes, packet sizes, network access methods, timeouts,

[23]There are other internetworking devices beyond those discussed in this appendix. For example, repeaters, routers and protocol converters are also means by which networks may be connected. Interested readers are referred to References 11, 14, and 26 for a full treatment of internet connectivity devices.

error checking, user access control, and status reporting between nets[Ref. 26, Ref. 30]. The technical complexity of accomplishing effective network connections is directly related to the degree to which the networks differ. Similar networks are fairly simple to connect while dissimilar networks require more complex solutions.

There are a variety of means by which local area networks may be connected. Bridges and gateways are the methods most applicable to NMPC's internet requirements. They differ in technical complexity and are used under distinct circumstances. Bridges function primarily at OSI's Layer 2 to store and forward frames between homogenous LAN's; whereas, gateways perform Layer 3 functions to store and forward packets between dissimilar networks. [Ref. 11:p. 324]

1. Bridges.

Bridges are far simpler to implement than gateways. Since they are used to connect homogeneous LAN's, they do not require as complex hardware and software as gateways do. The functions they perform are very basic, consisting primarily of receiving frames transmitted on one network and passing them to another. Some common bridge design characteristics are as follows [Ref. 26:p. 454]:

- Bridges do not modify the content or format of frames, nor do they add additional header information.
- Bridges should have adequate buffer capacity to temporarily store frames when they arrive faster than they may be forwarded.

- Bridges must contain addressing and routing intelligence in order to determine which frames to copy and forward on each network.
- Bridges may connect more than two networks.

Bridges are most often found connecting local area networks which comply with IEEE 802 standards [Ref. 11:p. 325]. With the exception of the HYPERbus, only 802.3 LAN's are used within NMPC; therefore, the remainder of this discussion will focus on bridges of this type.

In order for a bridge to function it must be able to identify which data units to copy and transfer between networks. On 802.3 networks, a sending node addresses data frames with a destination address and broadcasts them across the transmission medium. Transmitted frames pass all nodes on the network and each node examines and copies those bearing its address. As a node on the network, a bridge must use some criteria for determining which frames to copy and forward. Several methods are possible. The simplest method for a bridge between 802 networks is to simply copy and forward all frames it receives. This is the method most frequently used in bridging 802.3 networks. Under a more complex, but less common method, the bridge copies the frames it receives and then compares the destination address to a routing table. If the address is for a local node the frame is simply discarded, if it is for a remote node the frame is transferred to the destination network and broadcast.

In order to better understand how the 802.3 bridge forwards traffic between networks, it is helpful to consider the process in terms of the layers of

the OSI model and the sublayers identified under IEEE 802 standards. In general, OSI provides that routing functions will occur at Layer 3, the Network Layer. However, in 802.3 networks, transmissions are broadcast to all stations and bridges normally copy and forward all received frames. Thus, the routing function in such nets is substantially trivial making the Network Layer "thin or nonexistent" [Ref. 11:p. 17]. Accordingly, when such networks are interconnected using a bridge, its functions are performed at lower layers, primarily within sublayers of Layer 2.

The 802 standard divides Layer 2, the Data Link Layer, into two sublayers: Logical Link Control (LLC) and Medium Access Control (MAC). In networks which meet 802.3 standards, node (station) addresses are found in the MAC sublayer of the Data Link Layer. Thus, bridges connecting 802.3 networks accomplish their functions within this layer.

In order to better understand the process performed by a bridge, consider the following example. Two 802.3 networks, A and B, are joined by a bridge. A node on Network A has traffic to transmit through the bridge to Network B. Figure F-1 on the following page uses the layers of the OSI Model (and 802 standards) to diagram the sending node, bridge, and receiving nodes for this example and is discussed below.

Data is encapsulated and transmitted across an 802.3 net as follows. Network A's sending node has traffic intended for a Network B receiving node. The traffic is divided into data frames (packets) by the station's upper layer(s).

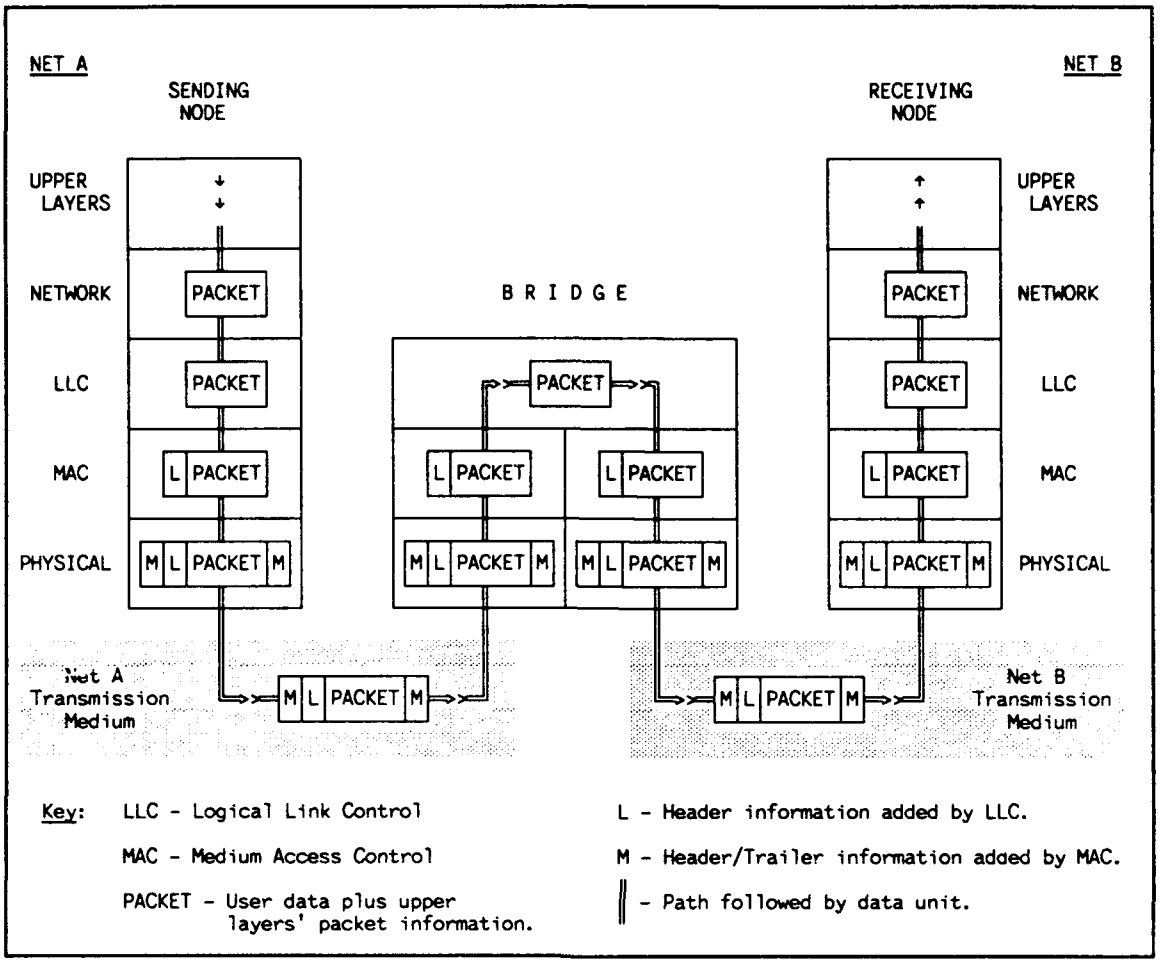


Figure F-1: Bridge

The data packet (frame) is then passed down to the LLC. The LLC adds its head to the frame and passes it to the MAC. The MAC encapsulates this data into a frame suitable for transmission across the network medium by adding a header and trailer to form a MAC frame. The physical layer receives the MAC frame and broadcasts it across Network A's transmission medium to all stations on the network. The bridge receives the frame on Network A's transmission medium and stores it in a buffer, if necessary, otherwise it processes and forwards it immediately.

When received by the bridge, the frame is passed from the physical layer of the sending net's side of the bridge up through the MAC and across the LLC which passes it down through the MAC of the receiving net's side of the bridge where it is re-encapsulated. It is then passed to the physical layer for broadcast across Network B's transmission medium. The Network B receiving node recognizes its address and copies the frame. There the frame is passed from the physical layer up through the MAC layer where the MAC header and trailer are stripped off and then to the LLC where its header is removed. It is then passed to the node's upper layers for further decoding and use. [Ref. 11, Ref. 26]

This example shows that a bridge between 802.3 networks forwards data through a straightforward process. 802.3 bridges are relatively simple to implement and are widely available off-the-shelf from a variety of vendors. Because bridges are relatively free from complexity, there are several advantages in their use; however, they may only be used to connect similar or homogeneous networks. Dissimilar networks must be connected using gateways.

2. Gateways.

Gateways are far more complex than bridges. They are often difficult to implement and may or may not be readily available on the commercial market. Although gateways between common systems are often available, unusual gateways must normally be custom built and in some cases may not be possible to implement. Since gateways are used to connect dissimilar LAN's

they require much more complex hardware and software than do bridges. Gateways must perform sophisticated functions to reconcile differences in the addressing schemes, packet sizes, network access methods, timeouts, error checking, user access control, and status reporting between the networks they connect. [Ref. 26]

Gateway functions are performed in Layer 3, the Network Layer of the OSI model. When necessary, this layer may be further divided into three sublayers: the subnet access, subnet enhancement, and internet sublayers. These provide the services necessary to accommodate various differences between the networks (subnets) being connected by the gateway. The subnet access layer provides the network layer protocol and services for the specific type of subnet being used. The subnet enhancement layer works to reconcile differences between the services offered in the subnets the gateway connects. It offers the services necessary to adjust the characteristics of its subnet's frames to meet the requirements of the internet layer (or conversely to adjust the internet frames to the characteristics of the subnet). Figure F-2 shown on the next page depicts the position of these sublayers in the context of the OSI model as they would be found in a typical gateway connection between networks. The following discussion explains the process represented by this figure. [Ref. 11]

A data frame originating on Network A moves down through the OSI layers and in the process is encapsulated according to its network requirements.

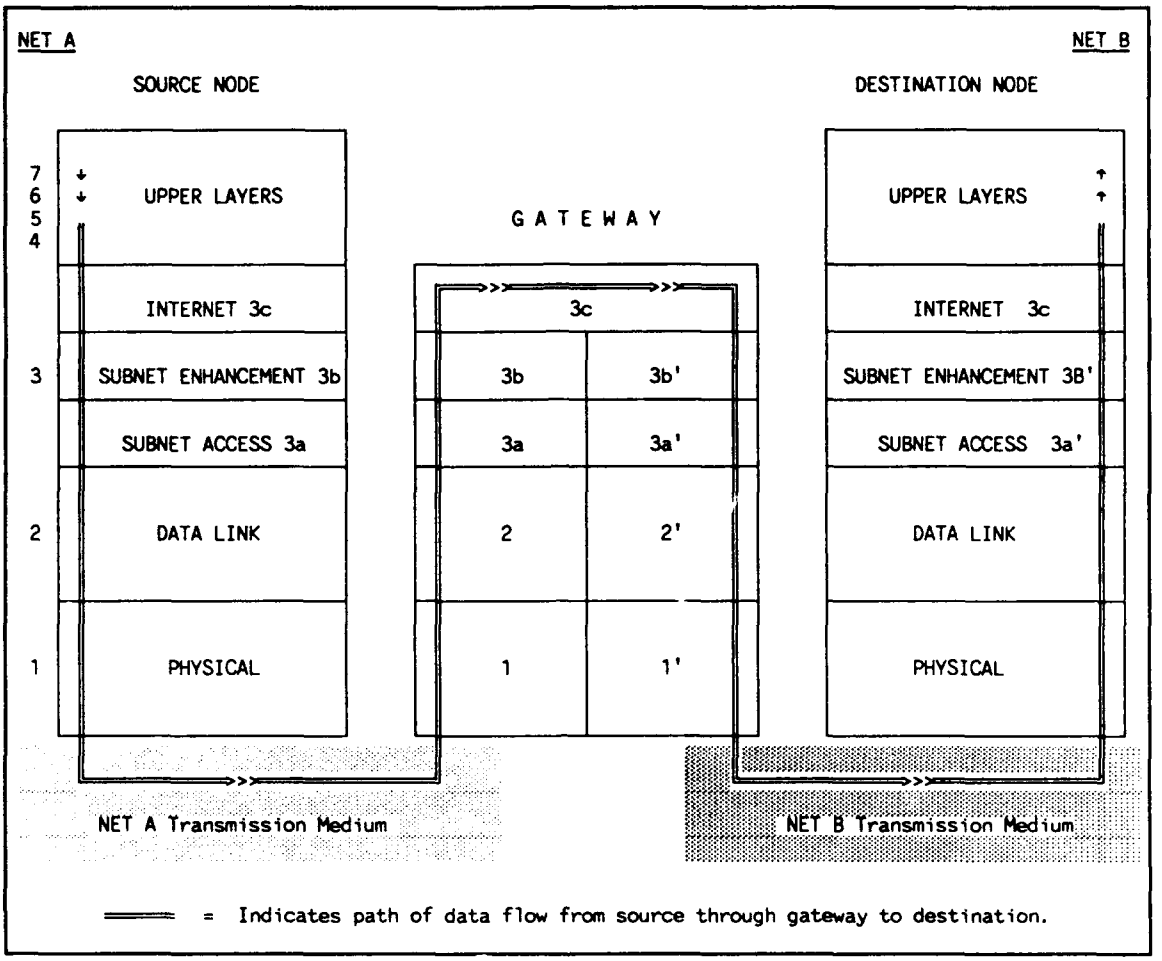


Figure F-2: Gateway

The resulting frame is sent across Network A's transmission medium to the gateway. Upon receipt by the gateway, the frame moves up through the Network A OSI layers and is progressively stripped of headers and trailers to reach the subnet access layer. This layer provides services to Network A's subnet enhancement layer where the frame is manipulated as necessary to prepare it for the shared internet sublayer. The internet sublayer uses a protocol format common to both the source and destination networks and allows the frame to be passed to the subnet enhancement layer of Network B. There it

is transformed into a frame format meeting the unique requirements of Network B. The Network B subnet access layer then receives the frame, modifies it, and passes it down through Network B's lower layers for transmission across the destination medium. Upon receipt by the destination station, the frame is passed back up through Network B's OSI Layers for decoding and use. [Ref. 11]

The processes presented in this example are typical of a gateway; however, the manner in which a gateway performs these functions varies according to whether it is of a connection-oriented or connectionless type. OSI allows for each of these. There are advantages and disadvantages of each type under different circumstances. For example, connection oriented gateways are normally used in connecting LAN's and WAN's; whereas, connectionless gateways are most often found in connecting LAN's to LAN's [Ref. 11:p. 337]. NMPC's requirements to connect diverse LAN's which implement similar architectures (CSMA/CD - CSMA/CA over ethernets) make connectionless gateways of primary interest in this study. Hence, connection-oriented gateways will not be discussed further here.[24]

Connectionless gateways are normally implemented using the ISO Internet Protocol (ISO IP) or an equivalent one. Since ISO IP meets GOSIP requirements (Appendix E), the following gateway description assumes its use.

[24]Interested readers are referred to Tanenbaum for a detailed discussion of connection-oriented gateways in comparison to connectionless gateways.

In a connectionless gateway, the Transport Layer may expect the Network Layer to provide limited service which only allows it the ability to insert datagrams onto the subnet. Messages which exceed the maximum size of the network's datagram are divided into a series of datagrams for transmission across the net. As shown in Figure F-3 (adapted from Ref. 11:p. 342), a message to be transmitted across the net originates in the upper layers of OSI and is encapsulated in a datagram built by the addition of appropriate headers as it is passed down through the transport, network, and data link layers to the physical layer for transmission across the net. Upon receipt by the gateway the

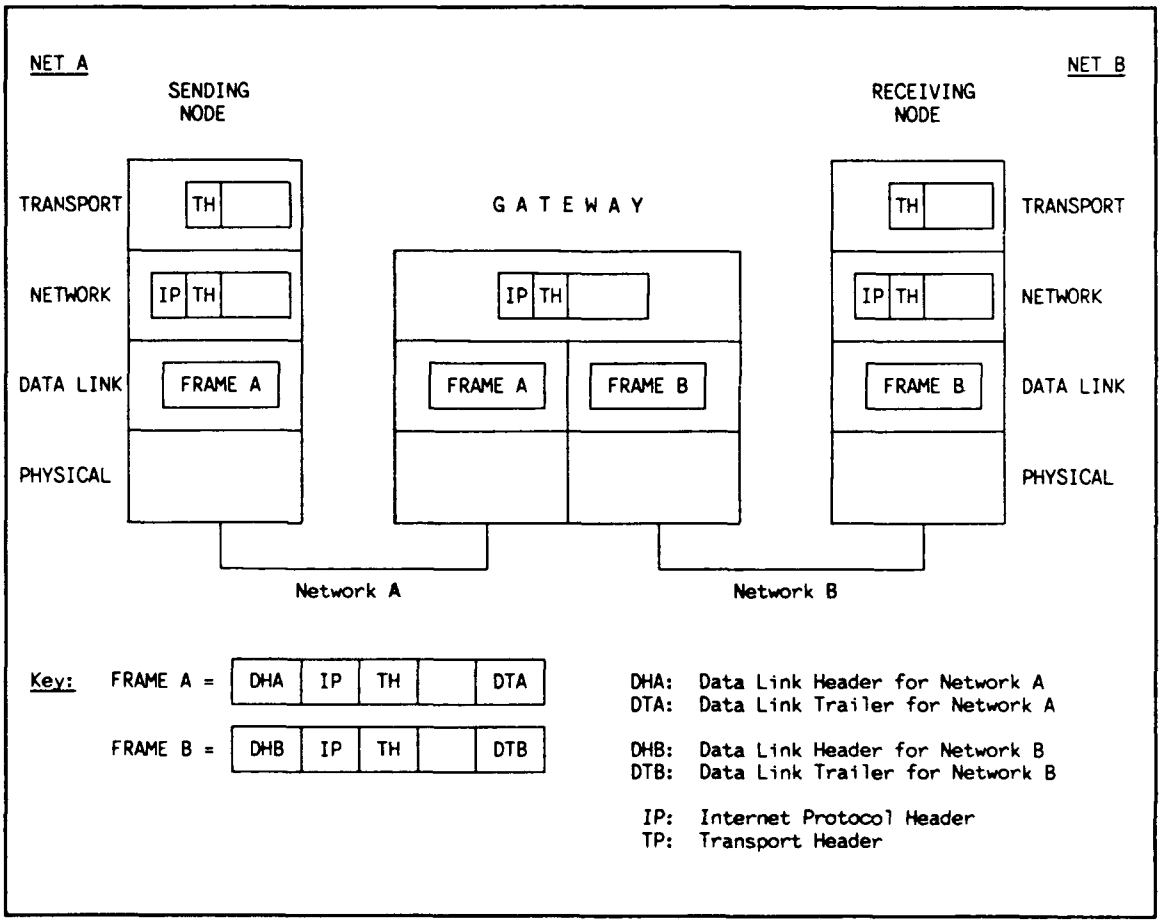


Figure F-3: Gateway Frame Conversion

datagram is stripped of data link headers and trailers as it is passed up through the layers to the Network Layer. It is passed across the Network Layer using the IP protocol and then moves down through the data link layer where it is encapsulated with header and trailer information of the format appropriate for the receiving network. It is then transmitted across the network to its destination where upon receipt it is passed back up through the lower OSI layers and transformed into the form appropriate for its upper layers destination. [Ref. 11]

Of course, addressing and routing functions are also performed as part of the process described above. Each gateway uses some form of routing algorithm to determine how a datagram is to be forwarded to its destination. These include adaptive routing algorithms which adjust routing paths to account for network conditions, fixed routing in which set paths are established for all given nodes upon initialization of the net, and flooding in which all received datagrams are automatically forwarded across the gateway (well suited to broadcast nets). [Ref. 11, Ref. 26]

In addition to performing routing functions and data frame conversions, gateways must also solve complex problems in reconciling differences in frame size between nets. Specifically, if the maximum packet size of one net is greater than that of the other, the gateway must manage frame fragmentation and reassembly. In other words, frames which have data sizes larger than those of the destination net will have to be divided into smaller frames and re-

encapsulated. This complicates the process of storing and forwarding data between nets because it requires that services be established to fragment and reassemble packets as required. [Ref. 11]

This raises the question of where the packets should be reassembled. An easy solution is to perform reassembly only at the ultimate destination; however, this means that datagrams may only retain their size or get smaller (and hence more numerous) as they move through the internet. A consequence of this is that the increased number of frames on the network may adversely effect its performance, particularly in the case of CSMA/CD nets. [Ref. 26]

It should be obvious from the above discussion, that gateways are complex entities which create additional overhead in network traffic and will slow the response time of transmissions across an internet. Therefore, gateways should be used to connect networks only when technical diversity among nets exists and there are no alternative solutions. Fortunately, NMPC's current network resources present several potential internet alternatives using both bridges and gateways in various combinations.

APPENDIX G: Characteristics of Selected Commercial Networks

A. INTRODUCTION.

This appendix discusses the characteristics and architectures of the commercial networks used or planned for use within NMPC. It is an adaptation and synthesis of a number of periodical articles, text discussions, and technical descriptions of DECnet, Novell, and HYPERbus networks as noted below. For readers who are unfamiliar with these commercial networks, this appendix will prove helpful in understanding the recommendations and discussion presented in 6, 7, and 8 of this paper.

B. DECNET.

Digital Equipment Co oration has been a leading pioneer in the development of effective network technologies.[25] In 1975, it produced its first release of DECnet which allowed directly connected PDP-11 computers to communicate with each other DECnet has evolved considerably in the 15 years which have passed since that first DECnet release. DECnet Phase IV has been in widespread use since its first release in 1984 and currently represents

[25]The DECnet discussion presented here follows closely the organization and content of Dennis F. Buss' articles "DECnet Architecture", "DECnet Address and Routing Functions", and "The DECnet Architecture and the OSI Model" which appeared in LAN Times, December 1989. It has been paraphrased, revised, and expanded to include material adapted from DataPro Research's article "Digital Equipment Corporation DECnet/Ethernet Products" published in April 1989.

significant improvements in functionality which make it a premier networking product today. Phase V DECnet is in its final stages of testing and will begin to be fielded this year (1990). In considering NMPC's networks, it is important to understand both DECnet IV and V.

1. DECnet Phase IV.

The capabilities of DECnet releases I through III included internetwork routing capabilities, ability to support up to 1024 nodes, and protocol support for Digital's Data Communication Message Protocol (DDCMP). Phase IV DECnet includes and surpasses these features. Significantly, it includes full support of the Ethernet protocol standard and has routing capabilities to support networks of up to 64,000 nodes. It supports X.25 packet switched networks, the use of specialized communications servers for offloading communications from a VAX, and interoperability with IBM's SNA protocols.

Digital produces DECnet/SNA gateways consisting of both hardware and software products that provide a virtually transparent bidirectional exchange of data between DECnet and IBM SNA environments. DECnet/SNA gateways allow VAX-run applications programs to communicate in an IBM network using IBM protocols. Most significantly, DECnet IV allows DECnet terminals to emulate IBM terminals and access IBM applications such as time sharing operations and control systems. Under DECnet, a VAX can even process jobs for IBM mainframes and thus act as IBM remote job entry systems. Thus, under DECnet

IV there is an established capability to interact with IBM processors which makes it well-suited for use by NMPC.

Beyond DECnet IV's ability to work well with IBM environments, it exhibits great strength in its peer-to-peer networking nature. Since DECnet nodes have a peer relationship with each other, each node within the network may communicate with every other node without having to access a central controlling station. This reduces communications overhead and increases the network's performance efficiency. Each node can easily access applications and facilities across the net thus all nodes may be equally responsive to user requests.

DECnet's decentralized architecture is complemented by its exceptionally robust routing capabilities. Through dynamic routing DECnet minimizes the number of hops between nodes in the transmission of a packet by rerouting to avoid inoperable or inactive network devices whenever possible. This adaptive routing is especially useful in large internets and improves network reliability overall.

DECnet accomplishes task-to-task communications through its Personal Computing System Architecture (PCSA) which allows diverse processors (e.g. VMS and MS-DOS based systems) to readily exchange information with each other. For example, under DECnet a C program running on a DOS PC can make requests and exchange data with a COBOL program being run on a networked VAX.

Remote file and record access is also well supported by DECnet IV. The Digital Command Language (DCL) allows programs and users to access files on remote nodes or host computers. For example, a VAX user can access files on a PC using DECnet DOS or on another VAX on the network simply by including the name of the remote node in the DCL command. Similarly, DECnet has superior on-line communications abilities allowing users to converse over the net by use of a "phone" function in which a user may contact and exchange information with a user logged on another node.

Terminal emulation is also fully supported by DECnet IV. A user of a VAX or PC on the net can log onto remote processors and execute commands, utilities, and programs just as if he were using a hard-wired, direct-connect terminal. This terminal emulation capability is a powerful feature of the DECnet system well suited to NMPC's NHBS network processing requirements.

DECnet's problem isolation and network management functions are exceptional advantages of its use. Network commands allow system managers to add nodes to the network or isolate problems without having to shut the network down to do so. This is in sharp contrast to many SNA and PC based networks which often require extended network downtime to accomplish such functions. DECnet's special utilities allow the network manager to monitor the status of the net, isolate problems, and add new entries to routing tables without disrupting the network. On VAX based nets, this is accomplished through the use of Digital's Network Management Control Center (NMCC)/

DECnet monitor -- a low overhead application which collects network data through node polling and remote event logging. Uploading and downloading of the memory contents of remote nodes to other nodes in the system can be accomplished when it appears a node is failing. This allows normal operations to continue while corrective measures are undertaken and makes DECnet one of the most robust network architectures available today.

2. DECnet IV and OSI.

For all its strengths, DECnet IV is only close, but not fully compliant to OSI standards [Ref. 15]. It has 8 layers rather than the 7 layers of the ISO OSI Reference Model as shown in Figure G-1.

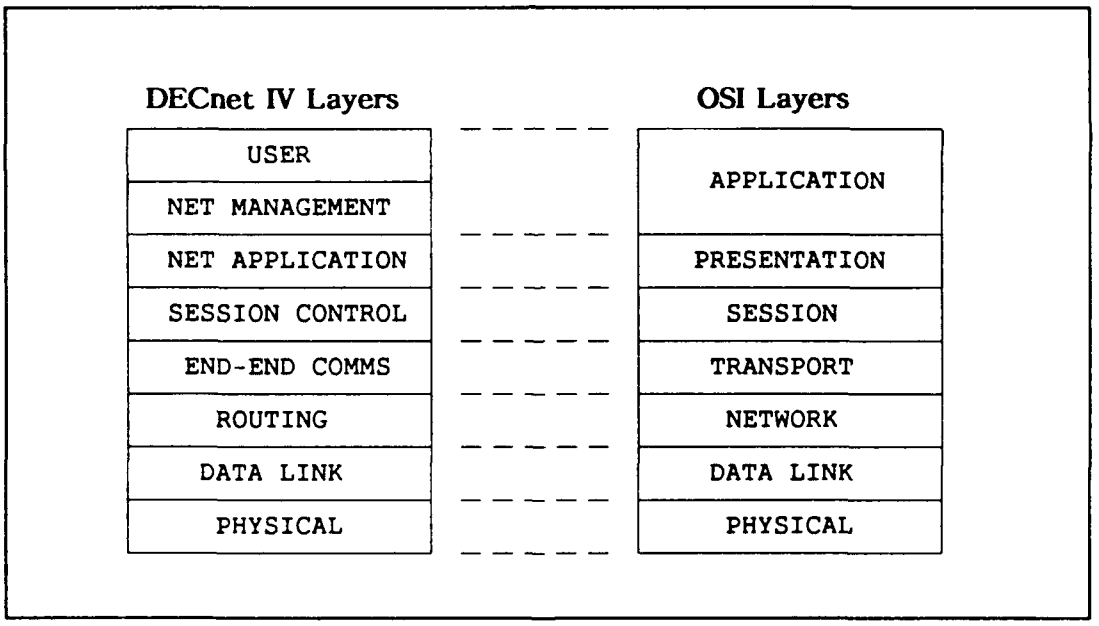


Figure G-1: DECnet IV - OSI Layers

In it's first two layers, DECnet exhibits exact functional correspondence to OSI's Physical and Data Link Layers. There is however a minor exception. Although DECnet IV, like OSI, supports Ethernet links in the Data Link Layers,

the protocol DECnet IV uses does not meet ISO's standards. The difference between DECnet's Ethernet implementation and that of the ISO standard lies primarily in the structure of individual data packets. The DECnet IV packet is not recognized by Ethernet devices that comply with ISO standards.

DECnet's next higher layer is called the Routing Layer. It performs the same functions as the OSI Network Layer; however, it uses different, incompatible packet routing algorithms to do so. The DECnet End-to-End Communications Layer corresponds to the OSI Transport Layer and performs similar functions of connection management, data flow control, end-to-end error control and message segmentation/reassembly; however, it does not use ISO protocols in doing so. DECnet IV's Session Control Layer corresponds to OSI's Session layer and is functionally compatible with it. At this layer, DECnet performs access control through the examination of logical link requests and the prevention of unauthorized resource access. It translates node names to net addresses and provides addresses for VAX processes.

The DECnet IV Network Application Layer handles remote file access, file transfer, remote terminal and virtual terminal functions, allows access to X.25 connections and to SNA gateways. It specifies network planning, controlling, and maintenance functions and is compatible with OSI's Presentation Layer. DECnet's two upper layers, the Network Management and User Layers, approximately correspond to OSI's Application Layer providing user level

services such as resource sharing, file transfers, remote file access, database access, and network management functions.

Although DECnet IV's 8 layers provide fairly exact correspondence to the 7 layers of the OSI model, DEC has designed its DECnet Phase V release to fully comply with the OSI standards.

3. DECnet V — Full OSI/GOSIP Compliance.

The impending release of Phase V will improve DECnet's capability as a truly open system networking architecture. It is fully compliant with the first four layers of the ISO OSI model and DEC is committed to its expansion to meet the protocol suite of OSI's upper three layers once ISO has completed their writing and approval. DEC recognizes that the integration of diverse PC LAN's into corporate-wide internets will be a principal 1990's market. Therefore, it has engineered DECnet V to facilitate internetworking through compliance with OSI standards.

The DECnet Phase V Physical Layer provides for the transmission and reception of individual bits forming higher-level messages across a physical medium (e.g. Ethernet). Its detailed operation complies with physical standards such as EIA RS-232 and the CCITT V.24 and X.21. The DECnet Data Link Layer provides dependable communications paths between a network's directly connected systems. To accomplish this, it defines three protocols: Digital's DDCMP, the high-level data link control (HDLC) protocol, and the ISO standards for Ethernet networks (ISO 8802-2, 8802-3). These protocols accomplish

backward compatibility to DECnet Phase IV (through DDCMP), OSI X.25 compatibility (via HDLC), and compliance with IEEE 802 standards for local area networks (through 8802-2, 8802-3). Thus, DECnet V will provide compatibility both with DECnet IV's older Ethernet standards as well as with current OSI standards.

DECnet's Phase V Network Layer will route user data between network systems through the use of the ISO Internet Protocol (ISO 8473). Implementation of this protocol will be accomplished in the communicating systems and routers which together join to form the network's data links. DECnet V's routing database will use the Network Layer to route data. Its architecture uses an adaptive routing algorithm to access the routing database and adaptively route packets to fit the network's topology. DECnet V's routing algorithm is so powerful, that it is designed to allow for networks of several hundred thousand systems. The DECnet Network Layer will also provide for using various kinds of communications including LAN's, synchronous circuits, X.25 networks, and internetworking with diverse vendors' networks which are OSI compliant.

DECnet V's Transport Layer, performs the OSI Layer 4 function of providing reliable end-to-end service between communicating systems with a transparent user interface. The two principal protocols used at this layer are the OSI Transport Control Protocol (TCP, ISO 8073) and the Network Services Protocol (NSP). The Transport Layer provides for recovery of lost data through

retransmission of undelivered packets and provides for the segmenting/ reassembly of user messages. It also accomplishes flow control matching the transmission and reception rates of packets while bypassing congestion using information from the network layer.

Although the OSI upper layers (Session, Presentation, Application) are not yet completely defined, DECnet's corresponding upper layers make full use of some standardized applications protocols, such as the X.400 message system and the File Transfer, Access, and Management (FTAM) standards. DECnet's Session Control Layer will be compatible with its Phase IV implementation as defined above. It will implement an expanded naming service to translate object names to network addresses for use by the lower layers. Access control restrictions will also be accomplished within this layer.

The DECnet V Application Layer allows the implementation of user defined applications for accessing and managing network resources. Applications available from DEC for this layer include network office systems, computer conferencing, remote database access, virtual terminal operations, SNA interconnection, network management, electronic mail, system services, and file transfer.

As is evident from the above discussion, DECnet V is designed to easily upgrade DECnet IV systems and meets OSI/GOSIP standards. This makes it a truly open system that is extremely well suited for use in meeting the challenges of internetworking requirements such as those of NMPC.

4. DEC's Ethernet and DECnet Address/Routing Functions.

With this broad understanding of the current DECnet architectures, we can now discuss some specific aspects of DEC's ethernet implementation and its DECnet address and routing characteristics. The DEC Ethernet implementation differs slightly from standard Ethernet specifications. It specifies digital, phase-encoded transmission over local, coax cable within limited distance requirements at transmission rates of up to 10M bps. Nodes are connected to the cable through a transceiver. Messages are broadcast over the Ethernet cable with the Data Link Layer at each station receiving all transmitted messages. Each node accepts and acts on only those messages addressed to it. Access to the net is controlled through CSMA/CD (discussed in Appendix B). Ethernet's high data rate makes CSMA/CD an effective contention management scheme since collisions are rare unless the network approaches near maximum capacity loading.

Ethernet's Data Link Layer produces frames that contain a synchronizing header, a six byte destination address, the data from the user message, and a 32-bit cyclic redundancy check. Valid frames contain at least 64 bytes. When a frame of less than 64 bytes is recognized as the result of a collision the receiving node ignores it and awaits its retransmission.

Digital's implementation of Ethernet allows both baseband and broadband transmission methods. Both allow high speed, peer communications links between nodes. Both can be used for file transfer, graphics, text,

facsimile data, and electronic mail. DEC baseband and broadband ethernets use the same communications controllers and various other compatible hardware devices.

Baseband Ethernet uses a ThinWire ethernet coaxial cable with only one channel on the cable. The broadband ethernet uses a multichannel cable. It uses frequency-division multiplexing to accomplish transmission of data across multiple channels over the same cable simultaneously. In this way it is possible to transmit data, video, and voice over the same wire. Broadband Ethernets can be implemented as single-cable networks with transmission and reception at different frequencies or as dual-cable networks where both transmitting and receiving are done at the same frequency on separate parallel cables.

DEC nodes are attached to baseband ethernets through a transceiver while nodes are connected to broadband nets through a broadband tap via a transceiver cable to a broadband transceiver. DEC uses unique clamping mechanisms making it possible to add and remove nodes from its ethernets without disrupting the network.

Addressing and routing functions are critical aspects of any network architecture. DECnet performs these functions through node addressing and routing based on a unique numeric address for every node within the network. Every node on an Ethernet network has a 48 bit address. 16 of these bits make up the DECnet address and a constant 32 bit number is appended when a system has loaded DECnet. Every manufacturer of Ethernet adapter cards or interfaces

has an assigned 32 bit block of addresses to use in giving each of its cards a unique physical address during manufacturing. This unique address is called the Ethernet hardware address. Since this address is found within the block of Ethernet addresses XEROX assigned to Digital, each Ethernet node address can be used as a DECnet node address.

DECnet addressing and routing functions are handled somewhat differently when multiple LAN's are tied together to form an internet. In such cases, the address for a DECnet node is composed of a 16-bit number. The first six bits make up the area address for the node and the last 10 bits are used to identify the node number within that area. Area addresses can be any number from 0 to 63 and node numbers may range from 0 to 1,023. This combination of unique area-node number combinations allows DECnet to support up to 64,000 network/internetwork nodes. Since it is unreasonable for a user to be expected to remember the numeric addresses of nodes, DECnet allows each node to define names for other nodes in the network. These names are mapped to numeric addresses in an address database managed by the session control software of the user's node. Each user's node may define its own names for other nodes in the net. These names may differ from node to node but will, through the database, be mapped to the correct numeric addresses. In this way, users on different nodes may use differing names to refer to the same numeric node addresses. Thus, when a user on the network requests access to a node by its name, the session control software consults its address database and translates the name

request to the correct numeric node address. This information is then passed to the end-to-end communications layer which establishes the logical link between the nodes.

In general, DECnet routing uses a node's numeric address in determining data routing. The DECnet routing layer determines the path from origin to destination that a data packet will take. Users need only specify the destination of messages, routing handles the details to ensure that data reaches its intended recipient. On a DECnet network, routing performs several functions: determination of the best path when multiple paths exist and adaptation to varied topologies and communications links. For example, if a packet is addressed to a local node, routing delivers it to that node; if it addressed to a remote node, it is sent to the next adjacent node for further forwarding.

In DECnet systems, the routing layer also performs maintenance and monitoring tasks. It adds counters to limit the life of packets, performs maintenance functions, collects network performance statistics, and buffers internet transmissions. The data gathering performed by the routing layer helps a network manager locate, identify, and correct network problems as a they first appear, thus preventing extended network downtime.

DECnets are uniquely well suited to large LAN implementations and the internetworking of multiple Ethernet LAN's. DECnet's ability to work in multi-vendor environments and intermix PC based networks with mini and mainframe

environments makes it an excellent candidate for use in meeting NMPC's internetworking requirements.

C. NOVELL NETWORKS.

Novell produces network products designed to complement a variety of network topologies and hardware produced by many different vendors.[26] Novell's NetWare products are designed to maximize the performance of PC based networks allowing easy station-to-station communications and broad support for diverse operating systems and off-the shelf applications. Novell offers NetWare to support star, strings of stars, token ring, and bus topologies. It supports multiple file servers, has powerful utilities, offers sophisticated help functions, provides electronic mail and text editing, and excellent security measures. Novell's electronic mail and messaging services are easy to use and have a text editor which facilitates message preparation.

NetWare provides a flexible, efficient networking environment which works well with diverse vendor hardware and system configurations. It is particularly known for its exceptional flexibility and speed. Through the use of memory caching, hashing, and elevator seeking routines, NetWare reduces processing time significantly. Memory caching eliminates disk access time for frequently

[26]The Novell discussion presented here follows closely the organization and content of Datapro Research's article "Novell NetWare Systems" published in June 1988. It has been paraphrased, revised, and expanded to include material adapted from Chapter 5 of Schatt's book, "Understanding Local Area Networks"; Hughes' article in the November 1989 LAN Times, "Novell Commits to OSI"; and an article entitled "TES 2.0 Links NetWare to VAX" in the January 1990 LAN Times.

used data by anticipating needs based on patterns of data requests and keeping most used programs/data in memory buffers for immediate access. Hashing schemes and elevator search routines reduce seek time considerably and make NetWare exceptionally fast in handling data retrieval functions in support of application programs and user requests.

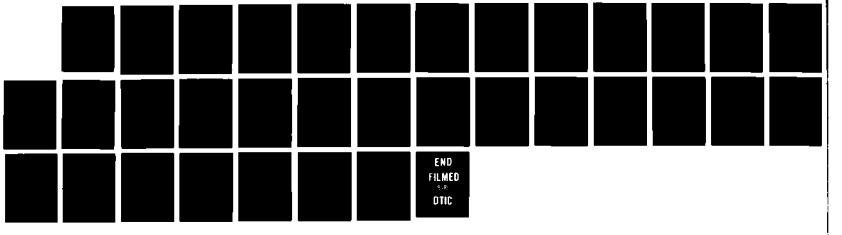
Another of Novell's strengths is its application programming interface which makes NetWare an open system allowing application developers to produce programs which make use of its well-developed multitasking environment. These value added services facilitate the functioning of sophisticated network applications and allow NetWare to work with a variety of hardware devices.

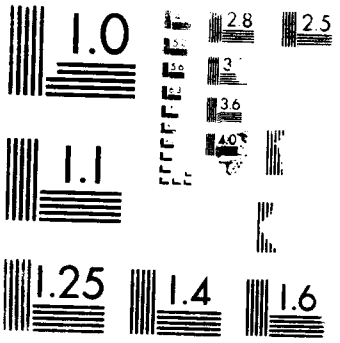
Novell offers NetWare SNA Gateway services which provide both IBM 3270 and 5250 emulations through PC gateway boards. Novell has well developed LAN-to-host connectivity services allowing peer-to-peer communications. Its NetWare Bridge software permits up to four dissimilar NetWare LAN's to communicate and share server resources in a manner transparent to the user. Novell also offers asynchronous communications servers which allow individual workstations to perform terminal emulation of Televideo or DEC VT100 terminals.

1. Overview of NetWare Architecture Today.

To better understand Novell networks and their role in meeting NMPC's internetworking requirements, it is necessary to closely examine the technical specifications of NetWare architecture. NetWare is built around the integration

AD-A230 334 A STUDY OF THE NAVAL MILITARY PERSONNEL COMMAND: 3/3
INTERNET CONNECTIVITY IS (U) NAVAL POSTGRADUATE SCHOOL
MONTEREY CA R E JOHNSON ET AL. MAR 90 XN-NPS
UNCLASSIFIED F/G 12/7 NL




1.0
2.8
2.5
3.2
3.6
4.0
1.1
1.25
1.4
1.6

of three software modules: the network operating system, the workstation shell, and bridge software.

The Network Operating System is a fully distributed, multitasking operating system. It provides network functions including directory and file services, print services, software protection, network security, and electronic mail messaging. The Advanced NetWare File Service Core Protocol (NCP) covers a variety of service calls forming the interface through which the workstation shells communicate with the operating system to provide network services for local applications.

The Workstation Shell provides a means by which a workstation's operating system requests are translated and mapped to network operating system functions. Novell's file server software resides in the application layer while the disk-operating software (DOS) resides in the presentation layer. The file-server software forms a shell around DOS. This shell intercepts applications program commands and translates them to network operating system requests as appropriate. The process occurs in a manner transparent to the user. Figure G-2 on the following page depicts the network interface shell.

The Bridge Module allows multiple network connections among dissimilar networks. NetWare bridges operate independently of communications media and communications protocols allowing both local and remote interconnections.

NetWare complies with OSI's seven layer model through the use of various protocols. NetWare's relationship to the OSI model is as shown in

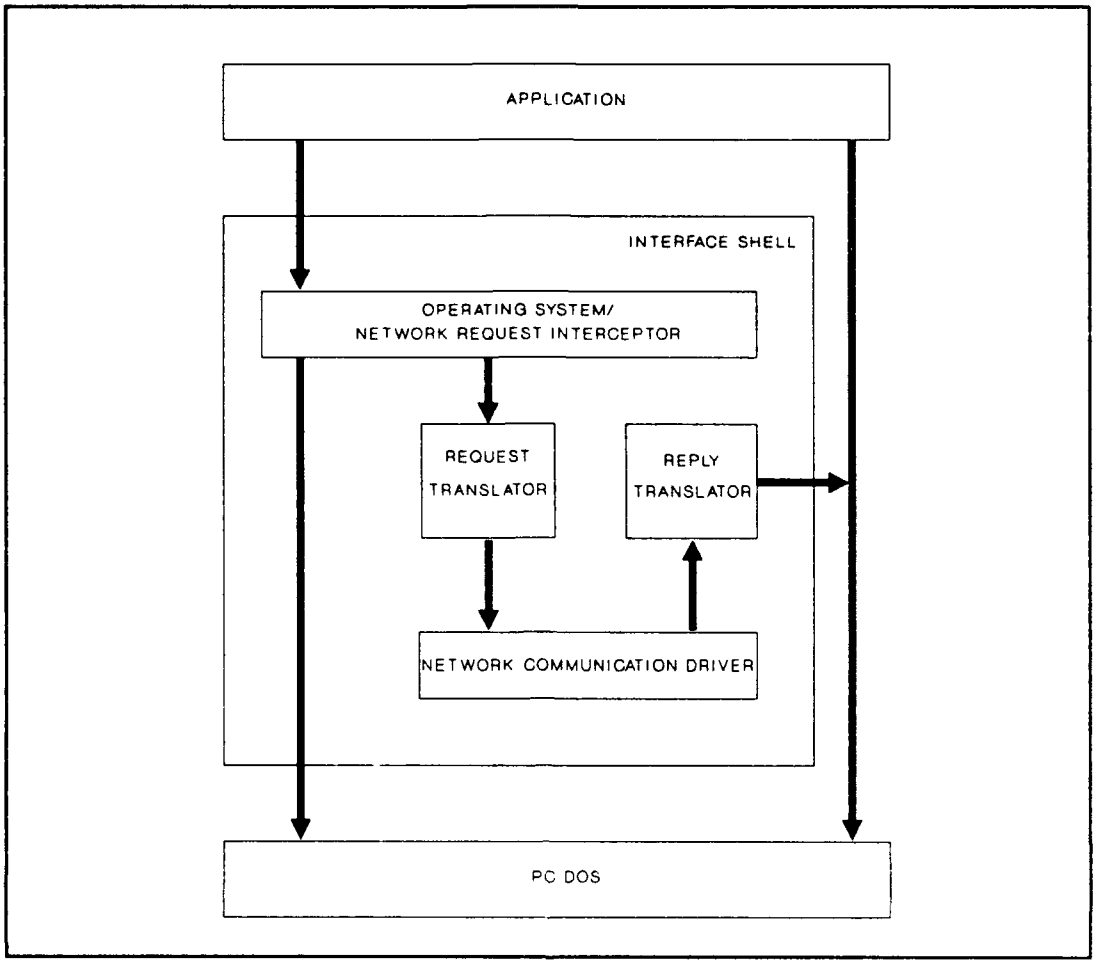


Figure G-2: Netware File Server Shell ***(Source: Ref 25:p. 121)***

Figure G-3 on the following page. NetWare has four distinct network interfaces. These are the datagram, virtual-connection, session, and workstation shell interfaces. The datagram interface is well suited for applications that have built-in delivery verification and error checking requirements. It provides simple, fast broadcast services that can be performed without the processing overhead of higher level interfaces.

The virtual-connection interface lies above the datagram interface. It provides guaranteed delivery of messages through positive acknowledgement of

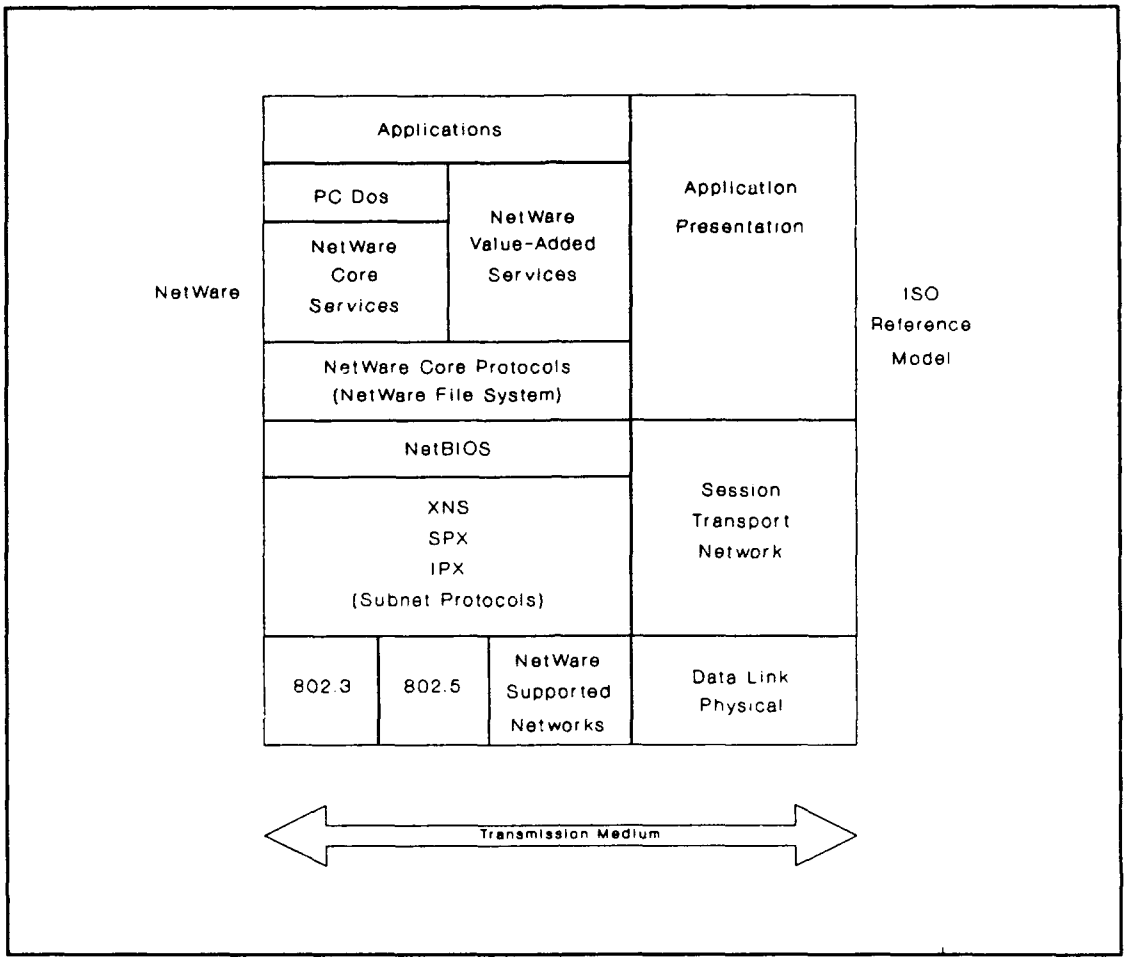


Figure G-3: Netware and the ISO OSI Model ***(Source: Ref. 6)***

packet transmission and receipt. When applications require optimal levels of communications performance and guaranteed message delivery, then the virtual connection interface is where the applications should be developed.

The session interface is built upon the datagram interface and lets network applications designed for the IBM PC LAN NETBIOS interface to run under NetWare without revision. The workstation shell interface maps DOS requests onto NetWare primitives to allow file service compatibility transparent to an application program. Together, the datagram interface and workstation

shell provide network access and advanced network services to most off-the-shelf applications.

NetWare consists of both standard and proprietary components. For example, the workstation shell and session interfaces conform to DOS and NETBIOS standards while the datagram and virtual-connection interfaces are Novell-specific. Netware's network layer, datagram interface is provided by the Internet Packet Exchange Protocol (IPX). On top of the IPX is the Sequenced Packet Exchange Protocol (SPX). SPX provides a guaranteed delivery interface for reliable message exchange in sequenced packet communications. IPX and SPX are based on Xerox' Internet Datagram Packet Protocol (IDP) and Sequenced Packet Protocol (SPP) respectively.

2. **Netware Operating System.**

The NetWare operating system provides a full suite of disk and I/O intensive operations. NetWare reduces operating system overhead by allowing for the completion of ongoing processing tasks before servicing incoming requests. It also implements a straightforward request/response interaction between client stations and resource servers requiring less code to execute basic tasks.

Internal bridging of up to four network adapter boards is possible with NetWare through the use of internal routers and LAN communications drivers at the bottom of the software layer. The internal router performs bridging functions between interconnected LAN's and manages host packets addressed to

the server. A set of communications driver specifications allows NetWare to support multiple network technologies independent of physical media and data link communications protocols. NetWare's communication specifications provide basic functions such as hardware initialization, packet transmission/reception, and error detection. Figure G-4 shows the internal communications layers of

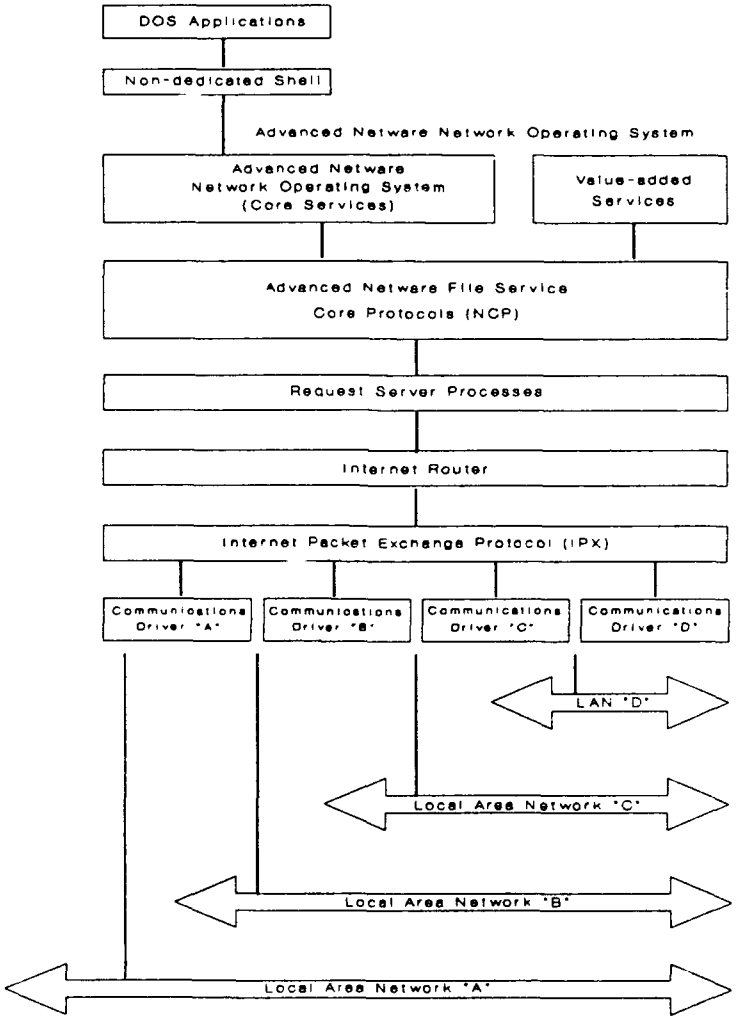


Figure G-4: Netware Communications Layers ***(Source: Ref. 6)***

the NetWare network operating system. NetWare uses a datagram protocol called IPX to allow applications running on its workstations to use network drivers and establish direct communications with servers and other network devices. IPX allows applications to send and receive individual packets across a NetWare network or internet. IPX's routing services work with NetWare servers and bridges to direct packets automatically between nodes in a manner transparent to the user even when accessing nodes residing on different networks. NetWare's internal router and request server work together to bridge multiple LAN drivers with communications packets. Incoming packets are taken off the LAN and transferred to a RAM server. The internal internet router then applies the appropriate algorithm to accomplish the routing of packets to specified locations. Client requests are processed with the highest priority being given to direct server requests causing necessary network primitives to be executed in order to complete the request and provide services.

The Netware File Service Core Protocols (NCP) layer is built upon a model of remote procedure execution and contains a set of service protocols defining client/server relationships. Requests sent to a server produce responses to the client. A service client builds a message containing all required parameters for transmission through the network messaging system to the server. The server performs the requested procedure and returns the results to the client. These core service protocols support the use of either IPX or SPX, with SPX being preferred for its guaranteed message delivery characteristics.

Server/client service begins with the establishment of a service connection. Although it is possible for a single connection to service more than one client request, current NetWare server implementations restrict a client to one outstanding service request per connection. When the server receives a new service connection request, it checks the current connection list. If a server-client connection already exists, then it is reinitialized and used to service the current request.

The NCP forms the basis of many NetWare services through its large set of data access and sychronization primitives listed by function as follows:

- Maintenance of service connections
- Directory maintenance
- Data access synchronization
- File maintenance
- Bindery (named objects) maintenance
- Print services
- Network management services
- System accounting services
- Software protection services
- Queue management services

Through NCP and these services the Novell NetWare environment is well suited to distributed processing. It has great flexibility to work with diverse operating systems since different operating systems can be mapped onto NetWare services.

NetWare also has strong network storage, printer management, and security capabilities. External disk subsystems may be added to Novell networks to increase available on-line storage and internal/external tape systems can be used to provide data backup. NetWare file servers can handle multiple printers (both serial and parallel) and allow users maximum printer control through easily accessible print spooling functions. Security may be separately managed for each server making Novell nets highly secure yet flexible in meeting user needs.

Novell's security features are much more advanced than most network operating systems. Netware allows access to be restricted to certain times, limits duration of access, can be configured to require passwords, establish user accounts with limited access, and lock out intruders. Network managers may use any combination of these security features to limit workstation, file server, file or program access. File server security can be managed in any of four ways and combinations thereof: Login/Password Security, Directory Security, File Attributes Security, and Trustee Security. The capabilities of the first three of these security functions may be inferred from their names. Trustee security requires more explanation.

Trustee security will normally form the majority of implemented system security measures. It allows the network security manager to set individual access rights for network users by controlling how they may work with files in a given directory. There are eight rights which may be granted or withheld using NetWare's Trustee security functions. These are as listed below:

- Read from open files
- Write to open files
- Open existing files
- Delete existing files
- Create/open new files
- Parental (control access rights to directories/subdirectories)
- Search directories
- Modify file attributes

Overall, Novell's NetWare offers sophisticated network management functions such as network monitoring, dynamic configuration, and flexible access restriction. It is a flexible, high speed system which uses efficient memory caching, buffering, and indexing schemes to reduce overhead processing time in performing network operations. It supports a wide range of network topologies and allows for multiple file servers, remote workstation access, bridges to other Novell networks, electronic mail, and powerful network security functions.

2. NetWare Communications Support Interfaces.

Advanced NetWare includes internetworking and connectivity capabilities which allow the interconnection of multiple networks. Novell supports the interconnection of networks through local and remote bridges, internet gateways, PC-to-LAN connections, and LAN-to-host interconnectivity. Using IPX as the common protocol, NetWare servers can interconnect dissimilar NetWare LAN's transparently. Additionally, Novell offers network hardware and

software to support several different bridges and gateways. Specifically, Novell provides four types of communications interfaces through NetWare: IBM compatible, IBM SNA gateway, TCP gateway, and asynchronous service interfaces.

The IBM compatible interface supports IBM's low level application program interface and micro-to-mainframe applications based upon IBM's API host interaction functions. The NetWare-SNA Gateway provides SNA services/ interconnectivity enabling networked PC users to communicate with IBM mainframe hosts. The TCP gateway is used to provide NetWare/TCP gateway, FTP, and Telenet applications through the use of an interface built upon the Berkeley Socket 4.2BSD interface. Novell's asynchronous interface is built upon the NetWare Asynchronous Software Interface (NASI) which provides simple and enhanced terminal emulation applications and the NetWare Asynchronous Command Interpreter (NACI) which provides session-level connection services.

Novell Netware may also achieve interconnectivity with DEC VAX systems on Ethernet LAN's through Terminal Emulation Services (TES) developed jointly by Novell and InterConnections, Inc. Using NetWare for VMS and TES, PC workstations on Novell LAN's may emulate interactive terminals such as VT220's, VT240's, VT320, Textronix, and others to log in to VAX/VMS systems and run applications. Additionally, TES includes a command line interface to allow DOS commands to be used in initiating and controlling VAX sessions.

Although NetWare has a wide range of network communications and internetwork options, it is primarily built on a proprietary basis and is only now moving toward full OSI compliance. As NetWare evolves to implement full OSI support, it will meet GOSIP standards and secure a leading role in government networking applications.

3. Novell NetWare, OSI, and GOSIP.

Novell has announced plans to achieve full OSI/GOSIP compatibility in 1990 as discussed below [Ref. 16]. NetWare Open Systems is Novell's architecture base for OSI compliance. When fully developed, it will offer a multi-protocol architecture that will provide Novell networks a basic OSI environment. It currently supports a variety of standards including TCP/IP, X.25, SNA, LU6.2 communications standards; IEEE 802.3 and 802.5 network media standards; NETBIOS, Named Pipes, Sockets, and IPX/SPX network application programming interface standards; and compliance with the ISO international data representation format standard (Abstract Syntax Notation version 1 -- ASN.1).

Novell's OSI architecture is consistent with both US and UK GOSIP. It extends the basic GOSIP architecture by use of an interface to an independent physical layer called the Open Data-Link Interface. This allows NetWare to simultaneously support different protocols through the same physical network interface. This will allow NetWare to achieve full interoperability with other OSI-compliant systems. At the Transport Layer, Novell has created the

Transport Provider Interface (TPI). TPI provides an interface between NetWare services and applications and a Unix environment.

Novell's commitment to OSI is well established. It is a member of the ANSI, IEEE and POSIX standards definitions committees and has played a role in the National Institute of Standards and Technology (NIST) X.400 and X.500 workshops. NetWare's RPC tools have been designed to allow developers to build distributed applications that are portable to OSI standards. This will allow applications currently written to run on top of IPX to be run over OSI transport protocols without any change. Clearly, Novell networks now enjoy a substantial degree of OSI compatibility which will continue to improve as Novell's 1990 release's are designed to achieve full OSI support.

D. HYPERBUS.

HYPERbus is a network built around a hierarchical bus structure of 75 ohm coaxial cable.[27] It uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as its contention method of network access control. NSC's CSMA/CA is essentially a virtual token passing scheme that maintains stability at high loads and provides predictable response times.

HYPERbus performs port selection and high performance multiplexing in connecting remote network terminals to mainframe hosts. Port selection is

[27]The Hyperbus discussion presented here follows closely the organization and content of NSC's "HYPERbus Systems Description Manual". It has been paraphrased and expanded with information provided by NMPC-167's HYPERbus technical personnel.

performed automatically; directing incoming connection requests to available host ports. HYPERbus multiplexing allows diverse speeds and protocols to be accommodated on its single cable communications circuits. Direct peer-to-peer communications are allowed between nodes without the need for intervening switching equipment; however, device protocols must be compatible in order for communications to occur. HYPERbus supports communications of RS232 and IBM 3270 terminal equipment at speeds of up to 10M bps.

1. **HYPERbus Components.**

HYPERbus networks consist of six basic components (see Figure G-5 on the following page): the bus coaxial cable, bus interface units (BIU's), bus tap units (BTU's), bus jack units (BJU's), dial pad units (DPU's), and bus service center (BSC). The HYPERbus transmission medium is 75 ohm coaxial cable which is used to form local buses which are then tied together to form a single HYPERbus network. It is a specially designed baseband coaxial cable supporting transmission rates of up to 10M bps.

Devices are connected to the HYPERbus coax through the use of Bus Interface Units (BIU's). The BIU's are the key element in HYPERbus connectivity. The BIU's are microprocessor controlled devices which handle data transmission on the network. Each BIU possesses enough processing capabilities to preclude the need for a central controller on the net. In response to a user request, the transmitting and receiving BIU's communicate to establish a circuit connection. The transmitting BIU generates a message frame which

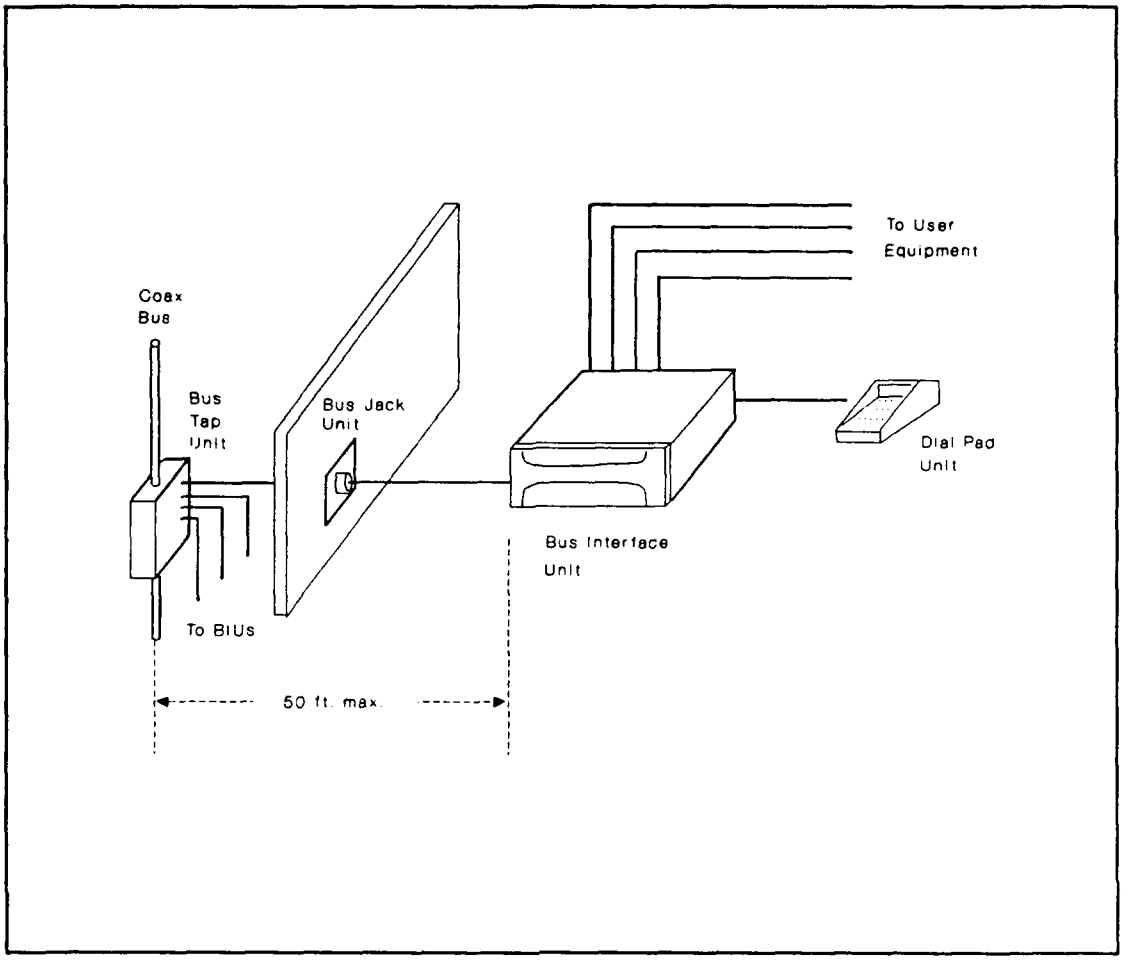


Figure G-5: HYPERbus Components ***(Source: Ref. 12)***

packages the user's data and sends it across the net. The source and destination BIU's communicate to verify correct transmission and retransmit if necessary. In addition to creating and controlling the transmission of frames, the BIU's track performance statistics such as number of frames transmitted and retransmissions required. There are four categories of BIU, each designed to meet the unique requirements of RS232, IBM 3270, minicomputer, and link applications respectively.

RS232 applications require the use of B100/B200 BIU's to interface standard synchronous and asynchronous user terminal equipment to the HYPERbus net. B100 series BIU's are used to provide direct attachment of RS232C equipment and host ports supporting data rates of 38.4K bps in full duplex communications. B200 series BIU's accomplish the connection of RS232C equipment through modems and dial-in communications.

IBM 3270 applications require the use of B300 series BIU's to provide connectivity of IBM 3270 equipment and controllers to the HYPERbus network. Using B300 BIU's, terminals may dial-in to an IBM host's 3274 controller or access alternate hosts without the need for separate switching hardware/ software.

Minicomputer applications require the use of B400 series BIU's to provide 16-bit direct memory access to the HYPERbus network. Using the B400 BIU's allows minicomputer hosts and subsystems to be interconnected allowing high speed resource sharing across the network using the HYPERbus message format.

Link applications use B800 series BIU's to interconnect constituent buses of a HYPERbus network into the overall hierarchical bus structure. They allow local bus networks comprised of diverse devices and BIU's to be interconnected into a single HYPERbus network. These link BIU's incorporate dedicated buffers allowing simultaneous virtual circuits between attached buses. Transmissions

are received and buffered by the link BIU and there await access through contention on the destination bus.

Bus Tap Units (BTU's) provide a tap connection to the bus coaxial cable and may accommodate up to four bus jack units (BJU's). They may be installed without cutting the cable or disrupting the network and form a passive interface to the bus. The BTU is connected to BJU's via shielded twisted pair cable of a maximum length of 50 feet. The BJU's are wall mounted outlets which allow users to unplug and move terminals as desired. Switches in the BJU define the tap's physical location and control its position in the contention timing scheme.

Dial Pad Units (DPU's) are devices used to initiate and check the status of BIU's. Each BIU has a port by which a DPU may be connected for profiling and diagnosing the status of the unit.

The Bus Service Center (BSC) is a monitor station for a HYPERbus network which provides four main functions: directory services, network BIU statistic tracking, security access for BIU control parameters, and maintenance/ diagnostic functions. BSC's enhance HYPERbus performance and may be placed throughout large systems to improve network maintenance and administration.

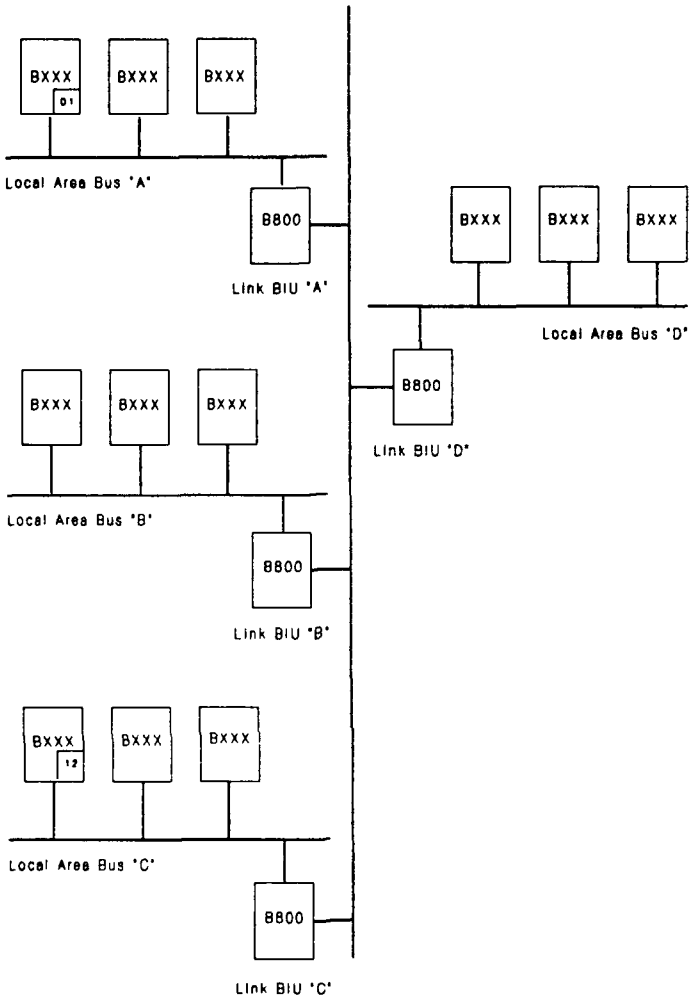
2. **Network Architecture.**

The topology of a HYPERbus network is a hierarchical bus of interconnected local buses. The maximum length of a local bus varies with the number of taps attached to it. They may range from a maximum of 4000 feet with eight BIU's hung from two taps to one thousand feet with 100 BIU's from

100 taps. Local buses are interconnected to form a comprehensive net by using link BIU's to connect them to a backbone bus. Transmissions confined to a local bus do not interact with the link BIU's. Inter-bus transmissions are done through the link BIU's as shown/discussed in Figure G-6 on the following page.

NMPC has a hierarchical HYPERbus consisting of 6 local buses connected through a central backbone. HYPERbus transmission protocols accomplish transmission across the bus in frames. Data is encapsulated in frames by the BIU and transmitted across the net. Each frame is made up of a header containing routing and priority information, a 16-bit cyclic checkword, and the body of data which together form a frame of up to 4K bytes in length. The bus protocol performs transmissions through frame-pairs and adheres to a specific frame sequence in order to ensure data integrity. When errors are detected, the appropriate frames are retransmitted. The entire process of frame generation and transmission is transparent to the user.

Although access to the coaxial bus is granted on demand through a CSMA/CA contention scheme, priorities may be established to control each BIU's access time. In this way, the network manager may prioritize bus access based on need and set each BIU accordingly. This scheme allows efficient use of bus capacity and yet preserves predictable response times even under high network loads. Each BIU may be assigned one of three transmission priorities: alert, normal, or background. Alert receives highest priority access to the net,



MULTIPLE LOCAL BUS CONFIGURATION

Traffic from BIU 01 on local bus A to BIU 12 on local bus C is buffered into link BIU A. Link BIU A contends for transmission on the backbone bus. Link BIU C accepts the transmission into its buffers and contends for transmission on local bus C, to BIU 12. BIU 12 then transmits it to the equipment at the receiving port. Transmissions between BIUs are transparent to the user.

Figure G-6: HYPERbus Multiple Bus Configuration *(Source: Ref. 12)*

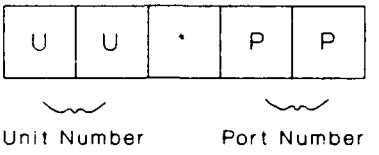
normal is as its name suggests, and background is the lowest priority with transmissions limited to avoid interference with alert and normal activity.

Addressing on the HYPERbus is accomplished through a hierarchical scheme corresponding to the topological structure of the net. HYPERbus addressing formats are shown in Figure G-7 on the next page. Each station on the net has a unique physical address as shown in Figure G-7 (a). In routing a transmission, a full network address is assigned which consists of the station and unit numbers of all link BIU's lying between the origin and destination stations as shown in Figure G-7 (b).

Transmissions on the network are accomplished through the establishment of a virtual circuit. A terminal dials a connect request through the terminal, host, or minicomputer as appropriate. The connect request must contain the addresses of all BIU's along the desired path. Establishing the path thus requires the intervention of the user, although once established it is transparent throughout the remainder of the communications session. Dialing a direct connection can become a complex task which requires the user to specify lengthy addresses incorporating the destination address as well as the addresses of all intervening BIU's. An alternative, is logical dialing which is available when the network includes a Bus Service Center (BSC). In logical dialing, the user may issue a simple dialing request in the form of a one to eight letter name which the BSC translates into the appropriate dialing sequence. HYPERbus also supports rotary dialing which attempts to access alternate,

G-7a.

Each station on the HYPERbus network is identified by a unique physical address:



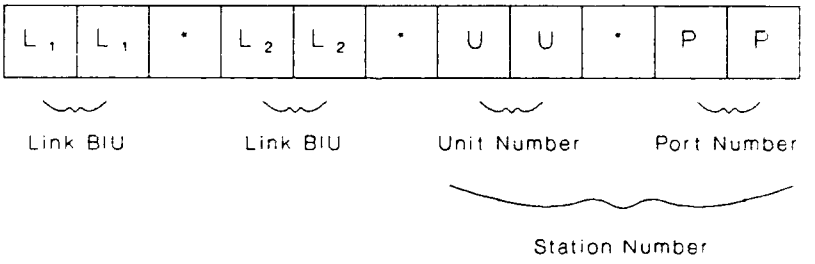
* = Separator

UU = the unit number of the BIU. This is the unit number that is dialed in to the switches on the back of the BIU.

PP = the number of the BIU port to which the equipment is attached.

G-7b.

A complete HYPERbus network connection address consists of the unit numbers of any link BIUs between transmitting and receiving BIUs, plus the address of the receiving station:



* = Separator

LL_1 = The unit number of the link BIU on the local bus.

LL_2 = The unit number of the link BIU on the backbone bus.

Figure G-7: HYPERbus Addressing Formats *(Source: Ref. 12)*

equivalent BIU ports when a primary port is found to be busy. Of course, this only works when BIU ports have been configured as equivalent when first installed in the net. It is useful when heavy use of particular stations is anticipated (for example, host-end front end processor connections).

3. Limitations of the HYPERbus.

By comparison to DEC and Novell network technology, HYPERbus is substantially obsolete. It has no OSI compliance, nor is it anticipated to have. According to NMPC technical representatives, NMPC's HYPERbus is one of only two such installations which remain in existence [Ref. 7]. It is bound by hardware and software limitations which make it a closed system, virtually inaccessible to OSI compliant systems. Research indicates that specialized hardware exists to partially overcome this limitation. For example, PC's may access the HYPERbus through the use of a specialized access card, produced by Chesapeake Computer Technologies.[28] The card allows IBM compatible PC's to be attached to BIU's and thus make use of the standard functions of the HYPERbus. Specifically, they may thus communicate with other HYPERbus network devices and access IBM mainframe applications. Although such cards allow PC's to be used as HYPERbus terminals, they do not overcome the other limitations of the network. HYPERbus uses a 75 ohm medium which is not compatible with the 50 ohm Ethernet standard and its routing and addressing

[28]The PI470 card is produced by Chesapeake Computer Technologies, 9101 Guilford Road, Columbia, Maryland 21046.

functions are heavily dependent on the HYPERbus specific hardware/software combination which governs network communications. HYPERbus is an older product for which there is little prospect of industry initiatives to overcome its limitations. In other words, efforts to achieve OSI interconnectivity or GOSIP compliance are not likely to occur unless the government specifically contracts for a unique solution. Overcoming the technical limitations of the net is problematic at best and not likely to be economically competitive given the rapid proliferation of standardized open systems network products now commercially available off-the-shelf.

APPENDIX H: SUMMARY OF NMPC OAN's/LAN's AND FUNCTIONAL REQUIREMENTS

DEPT	TYPE OF NET	OAN/LAN DEVICES				APPLICATIONS					ACCESS REQUIREMENTS		
		WS	PT	FS	CS	W	S	D	G	E	ODN	NMS	SEN
N-01 *	Novell, 802.3	40				✓	✓	✓	✓	✓	✓		
OP-01 *	Novell, 802.3	9				✓	✓	✓	✓	✓	✓		
N-02 *	Novell, 802.3	78				✓	✓	✓	✓	✓	✓	✓	
N-024	Novell, 802.3	27	3	2		✓	✓	✓		✓			
N-03 *	Novell, 802.3	60				✓	✓	✓	✓	✓	✓		
N-09 *	Novell, 802.3	1				✓	✓	✓		✓	✓		
N-2	Novell, 802.3	147	31	6	1	✓	✓	✓		✓	✓	✓	✓
N-4 *	Novell, 802.3	TBD				✓	✓	✓	✓	✓	✓		
N-6 *	Novell, 802.3	50				✓	✓	✓		✓	✓		
N-64	Novell, 802.3	66	3	2	1	✓	✓	✓	✓	✓	✓	✓	✓
N-663	Novell, 802.3	5	3	1		✓		✓	✓		✓		
N-7 *	Novell, 802.3	TBD				✓	✓	✓	✓	✓	✓		
N-83	Novell, 802.3	15	4	1		✓		✓					
OP-97	Novell, 802.3	45	10	2	1	✓	✓	✓	✓	✓	✓		✓
OP-11 *	3 Com, 802.3	6				✓	✓	✓	✓	✓	✓		
OP-13 *	Novell, 802.3	4				✓	✓	✓	✓	✓	✓		
OP-132▼	Novell, 802.3	30	10	2	1	✓	✓	✓	✓		✓	✓	
OP-136	Novell, 802.3	4	2	1	1	✓	✓	✓			✓		
OP-14 *	Novell, 802.3	2				✓	✓	✓	✓	✓	✓		
OP-15 *	Novell, 802.3	4				✓	✓	✓	✓	✓	✓		
N-16 *	Novell, 802.3	35				✓	✓	✓	✓	✓	✓	✓	✓
N-16R	Novell, 802.3	23	TBD	1	1	✓	✓	✓		✓	✓	✓	
N-163	Novell, 802.3	18	1	1		✓	✓	✓	✓		✓	✓ ▲	✓

KEY:

WS = Workstation
PT = Printer
FS = File Server
CS = Communications Server

W = Word Processing
S = Spreadsheet
D = Database
G = Business Graphics

E = E-mail
ODN = Other Departmental Nets
NMS = NMPC Mainframe Systems
SEN = Systems External to NMPC

NOTES:

* Based on interviews with LCDR Kuhn, NMPC-163, September 1989. Information limited to number of workstations and functionality. Although not specified, these nets also include printers, servers, etc. Complete info for other nets was taken from ASDP's.

▼ The workstations on this net are Macintosh's. A specially configured Z-248 is used as a communications server to meet NMPC's functional requirement for MS/DOS compatibility.

▲ This access is to the micro VAX 3600's of the NHBS system.

APPENDIX I: GLOSSARY OF ACRONYMS AND TERMS

Access Control - regulation of transmissions across a network to limit conflicts between nodes.

ADP - Automated Data Processing, the use of computer resources to process information.

ANSI - American National Standards Institute sets standards used by industry to foster compatibility among diverse vendor's products. ANSI standards are common to the computer industry and govern a wide range of programming and hardware attributes.

ASDP - Abbreviated System Decision Paper, a document used in the Navy's formal lifecycle management of an information systems development and procurement. The ASDP outlines the functional and technical requirements which must be met by the system.

Backbone - refers to a segment of a transmission medium used to connect a series of smaller segments (or networks) into a larger network (or internet).

Band-Aid - vernacular term implying a short term, temporary solution to a problem.

Baseband - transmission of signals without modulation. This scheme does not allow frequency-division multiplexing. [Ref. 26:p. 618]

Baseline Architecture - term used in the CNP TAP to refer to the existing technical architecture which forms the basis for the planning of transition and target technical architectures.

BIU - Bus Interface Unit, a microprocessor controlled device used in HYPERbus networks to handle data transmission across the network.

BJU - Bus Jack Unit, a plug on a HYPERbus network through which a BIU is connected to a Bus Tap Unit and thus to the network coaxial bus.

Bps - Bits per Second, a measure of the speed with which information is transferred.

Broadband - the use of coaxial cable for providing data transfer by means of analog (radio-frequency) signals. Digital signals are passed through a modem and transmitted over one of the frequency bands over the cable. [Ref. 26:p. 618]

BTU - Bus Tap Unit, a device used on a HYPERbus network to accomplish the connection of a BJU to the network coaxial bus.

Bus Topology - a topology in which a network's stations are linked in a linear fashion (or in the case of a hierarchical bus a series of linear links interconnected). (See Appendix B)

CCITT - International Consultative Committee on Telegraphy and Telephony, a UN treaty organization of member countries which establishes standards to facilitate the interaction of diverse international systems and products.

CDC - Consolidated Data Center, a Navy data processing organization located in Bratenhal, Ohio.

CIO - Chief Information Officer, term applied to the executive position envisioned by the CNP CIRMP to oversee the management of information as an integral part of overall strategic business management.

CNP - Chief of Naval Personnel, officer responsible for the overall management of all personnel functions and organizations of the United States Navy.

CNP CIRMP - Chief of Naval Personnel Component Information Resource Management Plan, the planning document governing IRM within the CNP claimancy.

CNP Claimancy - term applied collectively to Navy organizations performing the functions and responsibilities of the Chief of Naval Personnel.

CNP TAP - Chief of Naval Personnel Technical Architecture Plan, the planning document which outlines the baseline, transition, and target technical architectures for CNP information systems initiatives.

Coaxial Cable - a transmission medium. A cable consisting of one conductor, usually a small copper tube or wire, within and insulated from another conductor of larger diameter, usually copper tubing or copper braid. [Ref. 26:p. 619]

CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD - Carrier Sense Multiple Access/Collision Detection

DCNO - Deputy Chief of Naval Operations

DDN - Defense Data Network

DEC - Digital Equipment Corporation

DECnet - the trade name of DEC's network architecture.

DOD - Department of Defense

DON - Department of the Navy

DTE - Data Terminating Equipment

End User - an individual who uses information systems and applications in performing his work.

End User Computing - refers to information systems and applications development in which the end user plays a direct role.

Ethernet - a local area network and its associated protocol developed by Xerox and others. It is a baseband system. [Ref. 14:p. 225]

FCC - Federal Communications Commission

FIPS - Federal Information Processing Standard

Gateway - the hardware and software necessary to make two technologically different networks communicate with one another. [Ref. 14:p. 225]

GOSIP - Government Open Systems Interconnection Profile.

HYPERbus - a network produced by Network Systems Corporation and in use by NMPC. See Appendix G.

IBM - International Business Machines

IEEE - Institute of Electrical and Electronic Engineers.

Internet - a network formed by interconnecting two or more networks.

Internetworking - the process of building an internet of networks.

IRM - Information Resource Management

IS - Information System

ISO - International Standards Organization (See Appendix C)

LAN - Local Area Network (See Appendix B)

LLC - Logical Link Control (See Appendix D)

MAC - Medium Access Control (See Appendix D)

MAPTIS Grid - Manpower, Personnel, and Training Information System Grid, a communications grid of twisted pair wire running throughout the Arlington Navy Annex where NMPC is located.

MIS - Management Information Systems

MPT - Manpower, Personnel, and Training, used to denote Navy activities and organizations whose functions fall into these areas.

NETBIOS - Network Basic Input/Output System, a proprietary system originated by IBM and heavily influencing latter developments across the industry.

Netware - the name of Novell's primary network architecture/operating system.

NHBS - Navy Headquarters Budgeting System

NHPS - Navy Headquarters Programming System

NMPC - Naval Military Personnel Command

NMPDS - Naval Military Personnel Distribution System

Novell, Inc. - an industry leader in network products.

OAN - Office Area Network, as used in this paper synonymous with the term local area network. Denotes a LAN used primarily to perform office support functions.

Off-the-Shelf - existing technology which can be purchased commercially.

OPNAV - Operational Navy

Optical Fiber - a transmission medium which uses emissions of light to transfer data.

OSI Reference Model - Open Systems Interconnection Model

Peer-to-Peer - denotes a relationship between nodes of a network in which all stations have equal status.

POM - Program Objective Memorandum

PPBS - Planning, Programming, and Budgeting System, the methodology the Navy uses in allocating resources.

RAPIDS - Realtime Automated Personnel Identification System

RIOC - Remote Input Output Center

Ring topology - a physical arrangement of a network in which the transmission medium forms a closed loop. (See Appendix B)

Sunk Cost - term used to refer to costs which have already been incurred and should be considered irrelevant in the making of future economic decisions.

Technical Architecture - the configuration of ADP and communications hardware, software, and facilities required to support an organization's information processing requirements.

Thin Wire Ethernet - an ethernet built using RG-58 coaxial cable, a cable of less diameter and lower cost than that used in conventional ethernets.

Topology - the spatial pattern formed by the physical links of a network. [Ref. 27:p. 62]

Transmission Media - the physical links used to connect nodes in a network. (See Appendix B)

Twisted Pair - a transmission media of twin insulated intertwined copper wires. (See Appendix B)

VAX - a minicomputer produced by Digital Equipment Corporation.

Zenith 248 - an IBM-compatible PC produced by Zenith and a common standard throughout the Navy. Large numbers of Z-248's were procured by DOD under the first major umbrella contract for desktop PC's making it the de facto standard Navy PC.

LIST OF REFERENCES

1. Chief of Naval Personnel Component Information Resources Management Plan (CNP CIRMP), July 1989.

2. Mier, Edwin E., "LAN Gateways, Paths to Corporate Connectivity," Data Communications, August 1989.

3. Leigh, William E. and Clifford Burgess. Distributed Intelligence Trade-offs and Decisions for Computer Information Systems. Cincinatti, Ohio: Southwestern Publishing Company, 1987.

4. Chief of Naval Personnel Component Technical Architecture Plan (CNP TAP), May 1989.

5. Digital Equipment Corporation DECnet/Ethernet Products. Datapro Research Corporation, Delran, New Jersey, April 1989.

6. Novell Netware Systems. Datapro Research Corporation, Delran, New Jersey, June 1988.

7. Interviews between Mr. Gary C. Bean, NMPC-167, and authors, 25-29 September 1989.

8. Reitman, Robert P. Scientific and Technical Reports: MAPTIS Grid Evaluation. CRC Systems Incorporated. Fairfax, Virginia. January 1983.

9. HYPERbus configuration references, office working papers, NMPC-167.

10. Networks and Architectures, Datapro Research Corporation, Delran, New Jersey, December 1988.

11. Tanenbaum, Andrew S. Computer Networks, 2nd ed., Prentice Hall. Englewood Cliffs, New Jersey. 1988.

12. HYPERbus Systems Description Manual. Network Systems Corporation, Minneapolis, Minnesota, 1984.

13. Local Area Network Traffic Capacities. Datapro Research Corporation. Delran, New Jersey, January 1986.

14. Madron, Thomas W. Local Area Networks: The Second Generation. John Wiley & Sons, New York, 1988.

15. Buss, Dennis F. DECnet Architecture, "LAN Times," December 1989.

16. Hughes, Janet. Novell Commits to OSI, "LAN Times," November 1989.

17. Federal Information Processing Standard 146: Government Open Systems Interconnection Profile. National Bureau of Standards.

18. Micro USA. SMS Data Products Group, McLean, Virginia. 1989.

19. "Telecommunications Policy," NMPC-1672 memorandum, dated 27 June 1989 and interviews between Mr. Stanley Scarano, Project Manager/Senior Systems Specialist, NMPC-1673D1, and authors 25-29 September 1989.

20. Interview betwen CDR Carpenter, Branch Head, Office Systems, NMPC-163, and the authors 25-29 September 1989.

21. Interviews between LCDR Pamala Kuhn, Head of Office Systems Development Section, NMPC-1633E, and the authors 25-29 September 1989.

22. NMPC-163 Office Automation Hardware and Software Standards, office working/policy papers, NMPC-167.

23. NMPC-1633E Abbreviated Systems Decisions Papers for LAN's referenced in Appendix H.

24. Overview of Local Area Networks. Datapro Research Corporation, Delran, New Jersey, March 1988.

25. Schatt, Stan, Ph.D. Understanding Local Area Networks. Macmillan, Indianapolis, Indiana, 1987.

26. Stallings, William. Data and Computer Communications [2nd ed]. Macmillan, New York, 1988.

27. Florence, Donne. Local Area Networks: Developing Your System for Business, John Wiley & Sons, New York, 1989.

28. Designing an Ethernet. Datapro Research Corporation, Delran, New Jersey, February 1989.

29. "Government Networking Solutions", Touch Communications Incorporated, Campbell, California, 1989.

30. Internetworking and Interconnectivity Course, Information Engineering Institute, Falls Church, Virginia, 1988.

31. "TES 2.0 Links NetWare to VAX", LAN Times, January, 1990.

INITIAL DISTRIBUTION LIST

1. Dudley Knox Library, Code 0142 — 2
 Naval Postgraduate School
 Monterey, California 93943-5002

2. Office of Research Administration, Code 012A — 1
 Naval Postgraduate School
 Monterey, California 93943-5000

3. Defense Technical Information Center — 2
 Cameron Station
 Alexandria, Virginia 22304-6145

4. Department of Administrative Sciences Library — 1
 Code 54
 Naval Postgraduate School
 Monterey, California 93943-5000

5. Prof. Myung W. Suh, Code 54Su — 1
 Department of Administrative Sciences
 Naval Postgraduate School
 Monterey, California 93943-5000

6. Prof. Magdi N. Kamel, Code 54Ka — 1
 Department of Administrative Sciences
 Naval Postgraduate School
 Monterey, California 93943-5000

7. Naval Military Personnel Command — 2
 ATTN: NMPC-16
 Washington, D.C. 20370-5000

8. LT Robert E. Johnson, USN — 2
 DCA/JDSSC
 Code JWMC
 45335 Vintage Park Plaza
 Sterling, Virginia 22710-6701

9. USA Decision Systems Management Agency — 2
 ATTN: CPT Steven W. Peterson, USA
 Washington, D.C. 20310